6Ф2.39
С 80

СТАТИСТИЧЕСКАЯ
ТЕОРИЯ СВЯЗИ

ДЖ. ДЖ. СТИФФЛЕР

Теория синхронной связи

ВЫПУСК
3

621.39
С80

СТАТИСТИЧЕСКАЯ
ТЕОРИЯ СВЯЗИ

ДЖ. ДЖ. СТИФФЛЕР

Теория синхронной связи

ВЫПУСК
3

ДЖ. ДЖ. СТИФФЛЕР Теория синхронной связи

З. 5144-66 г.

621.39
С80

Дж. Дж. СТИФФЛЕР

Теория синхронной связи

Перевод с английского
Б. С. Цыбакова
под ред. Э. М. Габидулина

10
2025

058391

к
-2013

ИЗДАТЕЛЬСТВО «СВЯЗЬ»
МОСКВА 1975

ПЕРЕВІРЕНО

[illegible]ческая библиотека
Киевский
[illegible]ционный завод

621.39

6Ф0.1
С80
УДК 621.39.072.9

Ответственный редактор серии Б. Р. Левин

Редакционная коллегия:

А. Г. ЗЮКО, Л. М. ФИНК, Б. С. ЦЫБАКОВ, В. В. ШАХГИЛЬДЯН, Ю. С. ШИНАКОВ, Л. Н. ВЫЛЕГЖАНИНА

Дж. Дж. Стиффлер
С80 Теория синхронной связи. Пер. с англ. Б. С. Цыбакова под ред. Э. М. Габидулина. М., «Связь», 1975.

488 с., с ил., табл. (Статистическая теория связи).

Книга Стиффлера является пока единственной в мировой литературе монографией, в которой систематизирована и ясно изложена современная теория синхронизации систем связи. Теория синхронизации излагается на основе теории решений. Рассматривается синхронизация с помощью отдельного канала, а также непосредственно по последовательности сигналов, несущих информацию.

Книга рассчитана на широкий круг научных работников, инженеров, аспирантов и студентов старших курсов, специализирующихся в области передачи информации, вычислительной техники и кибернетики.

$С\frac{30401-035}{045(01)-75}$ 25—75 **6Ф0.1**

Theory of synchronous communications, Stiffler J. J.

Prentice Hall, Inc., Englewood cliffs, New Jersey, 1971.

$С\frac{30401-035}{045-75}$ 25—75

© Перевод на русский язык, издательство «Связь», 1975 г.

ПРЕДИСЛОВИЕ РЕДАКТОРА ПЕРЕВОДА

Книга Дж. Дж. Стиффлера «Синхронные системы связи» является пока единственной в мире монографией, в которой систематически излагается теория синхронизации систем связи. В книге собраны и обобщены результаты, разбросанные по многочисленным, зачастую малодоступным для советского читателя источникам. Отличительной особенностью монографии является рассмотрение проблем синхронизации в рамках общей теории кодирования, модуляции и оптимального приема сообщений. Такой подход позволяет естественным образом обнаружить тесную связь между весьма далекими, на первый взгляд, областями, как например, между теорией систем ФАПЧ и теорией корректирующих кодов.

В первой части рассмотрены вопросы, включаемые обычно в курсы под условным названием «Теория передачи сообщений». Интересны результаты, относящиеся к последовательному поиску. Кратко и ясно описаны дискретные по времени системы связи и системы ФАПЧ.

Во второй части рассмотрены собственно вопросы теории синхронизации, а в третьей — вопросы теории кодирования применительно к задачам синхронизации. Многие результаты в этой области принадлежат самому Дж. Дж. Стиффлеру, причем некоторые из них публикуются впервые.

Можно надеяться, что книга будет полезна советским читателям, желающим ознакомиться с современным состоянием теории синхронизации.

При переводе третьей (и частично второй) части были опущены доказательства ряда известных утверждений. Эти доказательства можно найти в литературе по теории кодирования, изданной в нашей стране. Кроме того, произведены сокращения вспомогательного материала (математических приложений, ряда задач, исторических замечаний и т. п.).

В заключение считаю своим приятным долгом поблагодарить Е. В. Воронова за помощь при подготовке перевода к печати.

Э. М. Габидулин

ПРЕДИСЛОВИЕ

Эта книга посвящена синхронизации в системах связи. На ранней стадии ее создания четыре последних слова составляли название книги. Настоящее название получило предпочтение по двум причинам. Во-первых, хотя книга посвящена исключительно системам связи, в которых для эффективной работы необходим синхронизм между передатчиком и приемником, рассмотрение, тем не менее, не ограничивается обсуждением только методов установления этого синхронизма; значительная часть книги посвящена описанию и исследованию самих систем связи. Во-вторых, некоторые вопросы, которые могли бы подпасть под первоначальное название книги (например, вопрос синхронизации *сети* в случае, когда некоторое число абонентов требует одновременного доступа к системе ограниченной емкости), здесь совершенно не исследуются.

Цель книги — изложить основы теории синхронных систем связи, принципы их функционирования и характеристики, а также представить выводы теории в форме, удобной для использования при проектировании систем связи. В соответствии с первой из этих задач теоретические вопросы излагаются достаточно подробно и приводятся доказательства всех наиболее важных результатов. Для решения второй из указанных задач при теоретическом рассмотрении упрощающие предположения вводились в тех случаях, когда только с их помощью можно было получить поддающиеся интерпретации результаты (т. е. те, которые можно объяснить без обращения к большим вычислительным машинам).

Книга состоит из трех частей. В первой части (с первой по пятую главы) излагаются основы статистической теории решений и статистической теории оценок; они применяются для анализа некоторых синхронных систем связи. Рассматривается также ряд дополнительных вопросов, в том числе теория поиска и теория систем фазовой автоподстройки частоты несущей (ФАПЧ), которые важны для второй части этой книги. Вторая часть (главы с шестой по девятую) посвящена методам установления синхронизма, необходимого для эффективной работы систем связи, описанных в первой части. В этой части даются ответы, по крайней мере, частично на вопросы: «каков наилучший метод синхронизации?», «насколько быстро можно войти в синхронизм?» и «с какой точностью можно поддерживать синхронизацию?». Третья часть книги посвящена теории кодирования и включает в себя как кодирование источников сообщения, так и кодирование для каналов связи. В соответствии с общей направленностью книги значительное внимание уделено методам построения кодов, дающих возможность установить и поддержать синхронизм между кодером и декодером.

В конце ряда глав имеются задачи. Эти задачи включены, главным образом, для того, чтобы расширить материал связанных с ними глав, а во многих случаях дать новый материал, который из-за отсутствия места не мог быть включен в основной текст книги.

Мы предполагаем, что читатель знаком с теорией случайных процессов и шумов. Для этого, например, вполне достаточным является материал первых девяти глав книги Давенпорта и Рута «Введение в теорию случайных сигналов и шумов» (изд-во ИЛ, 1960) или глав второй и третьей книги Возенкрафта и Джекобса «Теоретические основы техники связи» (изд-во «Мир», 1969). Для читателей с такой подготовкой настоящая книга будет содержать все необходимые для ее понимания сведения. Конечно, не следует думать, что привлечение дополнительного материала не рекомендуется, однако предполагается, что при чтении книги читатель с оговоренной выше подготовкой не почувствует необходимости обращаться к другим книгам.

Многим я хотел бы выразить свою благодарность за их помощь при подготовке этой работы. Прежде всего, это относится к моей жене, которая не только терпела мою работу над книгой в течение последних нескольких лет, но даже (чтобы отвлечь ее от мысли о требовании компенсации за мое преступление) была нагружена неоднократным перепечатыванием нескольких вариантов рукописи. Мне бы хотелось также особо поблагодарить профессоров Р. Штольца и И. Блэйк за чтение всей рукописи и за многие полезные предложения, способствовавшие ее улучшению. Кроме того, я очень благодарен профессору И. Блэйк за помощь при чтении корректуры книги. Я обязан также моим коллегам, которые либо добровольно, либо без сопротивления читали различные части рукописи и высказывали по ним свои мнения. К ним относятся доктора Е. Брукнер, С. Батмэн, Р. Эспозито, С. Фарбер, Р. Кинг, Дж. Лэйленд, Дж. Зальц, Г. Соломон и А. Витерби. Я особенно признателен доктору Р. Турину, оказавшему существенную помощь при последнем пересмотре рукописи, и П. Шоттлеру, который не только читал несколько глав рукописи и делал по ним замечания, но также прочитал корректуру верстки всего текста книги. Выражаю благодарность также Р. Холлу и Р. Джекобсону и их коллегам за участие в оформлении всех рисунков. Наконец, хочу поблагодарить профессора Т. Кайласа за предложение написать эту книгу и за ряд полезных предложений и критических замечаний на начальной стадии, а также профессора С. Голомба, который не только стимулировал мой начальный интерес к этой области, но и сам внес многое в решение проблем, рассматриваемых в книге. Кроме того, во время одного из периодически возникавших у меня приступов отчаяния из-за отсутствия прогресса при написании, в частности, глав рукописи, посвященных синхронизации, он обратил мое внимание на то, как уместны здесь слова Гамлета, которыми я заканчиваю это предисловие:

> «Порвалась дней связующая нить,
> Как мне обрывки их соединить!»
>
> *(«Гамлет», акт 1, сцена 5).*

Дж. Дж. Стиффлер
Конкорд, шт. Массачусетс

ЧАСТЬ I

ОСНОВЫ ТЕОРИИ

Глава 1

СИНХРОННЫЕ СИСТЕМЫ СВЯЗИ

1.1. Введение

Система связи может быть названа синхронной, если необходимым условием ее удовлетворительной работы является существование общего для передатчика и приемника отсчета времени. Цель вводной главы состоит в том, чтобы выделить характерные свойства таких систем и указать различные функции, которые может выполнять этот общий отсчет времени. Постепенно в дальнейшем будет выявлено отношение различных вопросов, обсуждаемых в последующих главах, к общей теории синхронной связи.

1.2. Модель системы связи

Структурная схема, изображенная на рис. 1.1, представляет собой обобщенную модель системы связи. Эта схема выбрана не только потому, что является достаточно общей и охватывает широкий класс систем, но также потому, что каждый ее блок предъявляет определенные требования к синхронизации, т. е. тре-

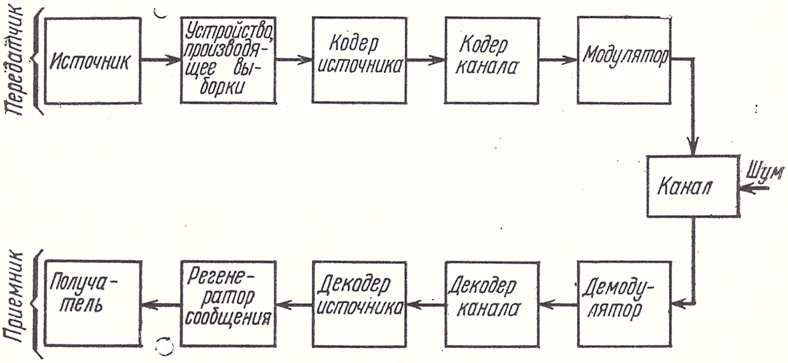

Передатчик
Источник
Устройство производящее выборки
Кодер источника
Кодер канала
Модулятор
Канал
Шум
Приемник
Получатель
Регенератор сообщения
Декадер источника
Декодер канала
Демодулятор

Рис. 1.1. Модель системы связи

бования, которым должен удовлетворять общий отсчет времени. Во многих системах отсутствует один или большее число блоков, указанных на рис. 1.1. Так как удаление какого-либо из блоков упрощает оставшуюся систему, то будем вначале рассматривать систему (имея в виду цели синхронизации), в которой присутствуют все блоки.

Источник представляет собой просто источник информации, которую нужно передать. Его выход, по предположению, является случайным процессом; он может быть непрерывным или дискретным по амплитуде, а также по времени. *Устройство, производящее выборки,* преобразует этот случайный процесс в случайную последовательность.

Кодер источника выполняет несколько функций. В наиболее простом случае он представляет собой преобразователь аналог-цифра, преобразующий поступающие на его вход выборки в последовательность цифр некоторой удобной системы счисления (например, часто, но не всегда, двоичной системы). В более общем случае он является устройством для отображения выборок в *слова,* т. е. в последовательности цифр или *символов*; это отображение может сильно отличаться от того простого отображения, которое обычно ассоциируется с работой преобразователей аналог-цифра. Кодер источника может быть предназначен, например, для того, чтобы снизить среднее число символов, необходимых для представления типичной последовательности выборок, с помощью уменьшения избыточности, почти неизбежно присутствующей в необработанных данных. Его функции могут определяться и какими-либо другими соображениями.

Как бы в силу иронии, *кодер канала* вводится для того, чтобы *внести* избыточность в последовательность символов, поступающую на его вход. Цель здесь состоит в том, чтобы дать возможность приемнику правильно опознать сообщение, представляемое теперь *кодовыми словами канала,* несмотря на некоторые ошибки, которые могут произойти при передаче. Оба этих кодера не нейтрализуют друг друга, как это может показаться с первого взгляда. Обычно естественная избыточность, устраняемая кодером источника, является намного менее эффективной в борьбе с ошибками при передаче, чем контролируемая избыточность, вносимая кодером канала. Даже если это и не так, уже то обстоятельство, что избыточность контролируется, позволяет использовать ее более рационально.

Функция *модулятора* состоит в преобразовании последовательности символов на выходе кодера в последовательность сигналов, пригодных для передачи по *каналу* связи. Каждый сигнал, в общем случае, содержит *несущую* (или *поднесущую*), обычно синусоиду, амплитуда, фаза или частота которой изменяются *(модулируются)* в соответствии с подлежащей передаче информацией.

Физические каналы часто можно представить как последовательное соединение устройства с некоторой частотной характеристикой $H_c(\omega, t)$ и элемента, который производит сложение сигнала с мешающим шумом. В последующих главах, когда будет необходимо указать более определенно тип канала, он всегда будет предполагаться широкополосным и не зависящим от времени, т. е. функция $H_c(\omega, t)$ будет предполагаться не зависящей ни от ω (в существенной для рассмотрения полосе частот), ни от t. Более того, обычно будет предполагаться, что шум представляет собой выборочную функцию белого (т. е. имеющего равномерную спектральную плотность на всех представляющих интерес частотах) гауссовского процесса. Получающийся в результате канал является удобной (но редко адекватной) моделью реального канала. (Возможно, что единственным физическим каналом, для которого все эти условия в действительности выполняются, является космический канал). Однако его важность обусловлена двумя следующими обстоятельствами: во-первых, его сравнительно просто анализировать; во-вторых, результаты этого анализа показывают, чего следует ожидать при исследовании более сложных каналов, и во многих случаях являются необходимой основой для получения более общих результатов.

На приемном конце действия производятся в обратном порядке; каждый блок (см. рис. 1.1) выполняет операцию, обратную по отношению к соответствующему блоку на передающем конце. *Демодулятор* преобразует принятые сигналы в последовательность символов, которую *декодер канала* переводит в тот вид, который, как мы надеемся, был на входе кодера канала. Затем *декодер источника* преобразует поступающую на его вход последовательность в последовательность импульсов различной амплитуды. Они, в свою очередь, используются *регенератором сообщения* для того, чтобы произвести вычисление оценки действительного входа источника, которая и поступает к *получателю.*

Описанная схема связи называется *дискретной системой связи с кодированием.* Если в схеме опущены блоки кодера и декодера канала, то система все же остается дискретной по своей природе (так как в ней используется лишь конечное число сигналов) и называется *дискретной* или *дискретной по амплитуде импульсной системой связи.* Если блоки кодера и декодера источника также отсутствуют, то система называется *непрерывной по амплитуде импульсной системой связи.* Хотя информация не имеет здесь дискретной формы (кроме того случая, когда сам источник является дискретным), все же до ее передачи еще производятся выборки (дискретизация по времени). Наконец, если устраняются также и устройство, производящее выборки, и соответствующее устройство на приемном конце, то система становится *аналоговой системой связи.*

При рассмотрении синхронных систем связи поучительно вначале предположить, что в действительности имеется общий отсчет времени, удовлетворяющий всем необходимым условиям. В соответствии с этим гл. 3 и 4 [следующие после вводной главы (гл. 2), в которой изложены некоторые основные понятия, необходимые для изучения систем связи] посвящены описанию и исследованию импульсных систем связи и, в частности, вида оптимального демодулятора для таких систем. Методы кодирования рассматриваются в гл. 10 и 13. Глава 10 посвящена вопросам построения кодов и устранения избыточности (кодирование источника), а гл. 13 посвящена вопросам борьбы с ошибками (кодирование для канала). Аналоговые системы, однако, здесь рассматриваться не будут, так как они обычно не являются синхронными и поэтому выпадают из круга вопросов этой книги. Если в аналоговых системах необходима синхронизация, то это неизменно связано с требованиями, предъявляемыми источником (как, например, при передаче телевизионных сигналов), а не самой системой связи[1]). Поэтому и метод, используемый здесь для синхронизации, также фактически не зависит от конкретно используемой схемы модуляции, а обсуждение этого метода не влечет за собой соответствующее рассмотрение оставшейся части схемы.

1.3. Задача синхронизации

Говорят, что две последовательности событий являются *синхронными,* если соответствующие события в них происходят одновременно. *Синхронизация* определяется просто как процесс установления и поддержания синхронного состояния.

Чтобы использовать эти понятия при рассмотрении систем связи, необходимо лишь положить, что одна из двух последовательностей событий, которые должны быть синхронизированы, имела место в передатчике, а другая — в приемнике. Обычно удобно как для понимания принципа, так и для работы разделить процесс синхронизации на два различных типа, хотя в некоторых случаях такое разделение довольно искусственно. Первый тип, *синхронизация отсчетов времени,* необходим для того, чтобы отсчеты времени, которые регулируют обе последовательности, подлежащие синхронизации (т. е. отсчеты времени в передатчике и в приемнике), производились с одной и той же скоростью[2]). Второй тип, *синхронизация более высокого порядка,* нужен для того, чтобы идентифицировать соответствующие пары событий в двух последовательностях и осуществлять их одновременное появление. Ясно, что если одно и то же событие происходит в двух одинаковых последовательностях одновременно и если последовательности развиваются с одной и той же скоростью, то последовательности являются и будут продолжать оставаться синхронизированными.

---

[1]) Следовало бы сделать исключение в этом утверждении для фазово-когерентных систем амплитудной модуляции. Несущая дает общий отсчет времени для передатчика и приемника, так что эти системы, по крайней мере, в некотором элементарном смысле, являются синхронными. В любом случае такие системы тесно связаны с системами когерентной амплитудно-импульсной модуляции, которые подробно изучаются в последующих главах, и поэтому не будут рассматриваться отдельно. (*Прим. авт.*)

[2]) В отечественной литературе «отсчеты времени» часто называются тактами, а «синхронизация отсчетов времени» — тактовой синхронизацией. Оставленный в переводе термин больше соответствует той общей концепции, которая развивается в книге. (*Прим. перев.*)

Если отсчеты времени в передатчике и приемнике достаточно стабильны, чтобы обеспечить требуемую точность синхронизации, то синхронизация отсчетов времени может быть опущена. Однако обычно этот случай не имеет места и для установления необходимой синхронизации отсчетов времени следует использовать подходящий метод. Самым прямым методом являются использование для отсчета времени в передатчике периодического сигнала и передача этого сигнала вместе с информацией. Соответствующим образом отфильтрованный принимаемый сигнал может быть затем использован для отсчета времени в приемнике. При таком подходе возникают два довольно фундаментальных вопроса. Первый вопрос, относительно структуры оптимального фильтра приемника, является предметом гл. 5. Второй вопрос, относительно взаимосвязи между используемым сигналом и качеством синхронизации отсчетов времени, рассматривается наряду с другими проблемами в гл. 6.

Конечно, сама несущая могла бы быть использована для отсчета времени. В *фазово-когерентной* системе[1]), в которой предполагается, что при демодуляции фаза несущей известна, должны также быть синхронизированы принимаемая несущая и местная опорная несущая. Если фаза несущей связана некоторым заданным и известным соотношением с отсчетом времени на передатчике, то местная опорная несущая также может быть использована для местного отсчета времени. Если передаваемый сигнал содержит спектральную компоненту на частоте несущей (т. е. если несущая не имеет 100%-ной модуляции), то возникающая ситуация будет такой, как описано выше. Однако, даже если такая компонента не передается, часто можно извлечь несущую из передаваемого модулированного сигнала. Соответствующие методы описаны в гл. 8. Заметим попутно, что синхронизация несущей является частным случаем синхронизации отсчетов времени, и поэтому она заведомо обсуждается в вышеупомянутых главах. В тех случаях, когда не требуется проводить различия, термины *синхронизация несущей* (или *поднесущей)* и *синхронизация отсчетов времени* будут использоваться как синонимы.

После того как отсчеты времени в передатчике и приемнике синхронизированы, начинается второй этап синхронизации. Некоторые события, происходящие в каждом из блоков на приемном конце схемы рис. 1.1, должны быть синхронизированы с соответствующими событиями, происходящими в аналогичных блоках на передающем конце. Для эффективной демодуляции необходимо, чтобы демодулятор был синхронизирован с модулятором так, чтобы было известно, когда кончается сигнал, представляющий один символ канала, и начинается другой *(синхронизация символов)*.

---

[1]) Системы, в которых работа демодулятора не основывается на знании фазы несущей, называются *фазово-некогерентными. (Прим. авт.)*

Декодер канала не может правильно работать до тех пор, пока он не сумеет определить начало каждого кодового слова (*синхронизация кодовых слов*). Аналогично декодер источника бесполезен, если поступающие на его вход символы не могут быть разделены на группы, каждая из которых соответствует выборке сообщения (*синхронизация слов сообщения*). Наконец, так как смысл любой конкретной выборки сообщения может быть определен лишь ее положением в последовательности выборок [или в *блоке (кадре)*, как иногда говорят], генератор сообщения часто должен быть синхронизирован с выборками сообщения (*синхронизация кадров*).

Если невозможно точно определить, происходит ли событие в момент t или в момент $t+nT_0$, где n — какое-либо целое число, то говорят, что существует *неоднозначность во времени*, равная T_0 секундам. Минимальная приемлемая неоднозначность во времени в системе связи равна периоду события, требующего синхронизации наивысшего порядка (т. е. периоду кадра). Если бы период отсчета времени был равен минимальной приемлемой неоднозначности во времени или равен некоторому целому кратному этой величины, то фаза принятого сигнала времени сама бы давала всю необходимую информацию о синхронизации и синхронизация второго типа была бы тогда избыточной. К сожалению, редко бывает разумным использовать отсчет времени, имеющий такой большой период. Таким образом, если период отсчета времени равен ΔT секунд, а минимальная приемлемая неоднозначность во времени равна T_0 секунд, причем $T_0/\Delta T \triangleq N > 1$ [1]), то остается N-кратная неоднозначность, которая должна быть разрешена, прежде чем процесс синхронизации будет считаться законченным. Цель синхронизации более высокого порядка состоит в том, чтобы выполнить это разрешение.

Как и в случае синхронизации отсчетов времени, очевидным методом передачи информации, необходимой для синхронизации более высокого порядка, является использование отдельного канала единственно для этой цели. Менее очевидный, но потенциально более эффективный подход состоит в попытке осуществить требуемую синхронизацию с помощью модулированных сигналов. Оба эти метода детально изучаются в последующих главах. Рассматриваемые задачи включают в себя: задачу синтеза сигнала в случае, когда используется отдельный канал для синхронизации (гл. 6); задачу оптимизации процедур различения гипотез и оценивания в применении к синхронизации для случаев, когда используется отдельный канал для синхронизации (гл. 6) и когда информация для синхронизации извлекается непосредственно из модулирующего сигнала (гл. 7). В гл. 9 рассматриваются вопросы о том, к чему приводит несовершенная синхронизация, и вопрос об оптимальном распределении мощности между синхроканалом и каналом для передачи информации. Наконец, гл. 11, 12 и 14 посвящены анализу методов внесения дополнительных ограничений на способ, которым символы, представляющие сообщение, группируются в слова с тем, чтобы появилась возможность синхронизации слов.

---

[1]) Символ $\triangleq$ используется в дальнейшем для обозначения равенства по определению. (*Прим. авт.*)

Прежде чем закончить эти вводные замечания, следует, возможно, сказать о методе, с помощью которого наиболее часто устраняются неопределенности во времени. Если каждый кадр содержит, скажем, n_1 слов, каждое слово содержит n_2 символов и каждый символ длится точно n_3 периодов отсчета времени и если эти числа n_1, n_2 и n_3 известны, то все требуемые типы синхронизации, в принципе, можно осуществить после того, как будет установлена синхронизация кадров. Отсюда следует, что нужно сосредоточить внимание исключительно на синхронизации блоков и получить всю остальную информацию о синхронизации как вторичный продукт. Это был бы разумный подход, если бы не было никаких ограничительных условий на сложность устройств, используемых на приемном конце; однако такой подход не практичен, когда нужно работать при более привычных ограничениях. Как будет показано, время, необходимое для разрешения N-кратной синхронизационной неоднозначности при типичных ограничениях аппаратурного характера, прямо пропорционально N и даже может быть пропорционально некоторой целой степени N в зависимости от обстоятельств. Таким образом, если $N=n_1n_2n_3$ и если следует разрешить всю N-кратную неоднозначность за одну операцию, то время синхронизации будет порядка $n_1n_2n_3$. В противоположность этому, если сначала устанавливается синхронизация символов, затем, соответственно, синхронизация слов и кадров, то время, необходимое для синхронизации, будет пропорционально $n_1+n_2+n_3$, т. е. полная задержка синхронизации равна задержке, необходимой для разрешения n_3-кратной неоднозначности в синхронизации символов, сложенной с задержкой для разрешения n_2-кратной неоднозначности в синхронизации слов и задержкой для разрешения n_1-кратной неоднозначности в синхронизации кадров. Если используется внутренняя подструктура, которая необходимо имеется в каждом кадре, то полное время синхронизации может быть снижено в (существенное) число раз: $n_1n_2n_3/(n_1+n_2+n_3)$. По этой причине наиболее разумно начать, вообще говоря, с синхронизации самого низкого порядка (т. е. с синхронизации для устранения наименьших неоднозначностей) и затем последовательно переходить к синхронизации более высоких порядков.

Глава 2

ПРОВЕРКА ГИПОТЕЗ, ТЕОРИЯ РЕШЕНИЙ И ПОИСК

2.1. Введение

Большая часть материала этой и последующих глав связана со следующей общей задачей. Наблюдается случайный процесс $y(t)$. В результате наблюдения выделяется множество координат или, проще говоря, *наблюдаемых*¹) $Y=\{y_i\}$. Известно, что эти наблюдаемые порождаются источником, который может находиться в одном из нескольких возможных *состояний.* Статистические свойства наблюдаемых предполагаются известными для каждого состояния источника. Требуется определить по этим наблюдаемым истинное состояние источника. Основные правила, по которым производится это определение, будут меняться. Иногда число наблюдаемых в множестве Y будет фиксированным. В других случаях число наблюдаемых будет существенно неограниченным, но решение должно быть построено на основе как можно меньшего их числа при условии, что задано ограничение на надежность этого решения.

Иногда ограничения на сложность аппаратуры будут требовать, чтобы решение было сделано в несколько приемов; возможно, что за один раз будет проверяться только гипотеза об одном состоянии. В других случаях гипотезы обо всех состояниях могут быть проверены одновременно.

В любом случае важными являются следующие вопросы: как при заданных основных правилах решения задачи наилучшим образом использовать находящиеся в распоряжении наблюдаемые, чтобы установить состояние источника; насколько надежным является окончательное решение.

В этой главе предпринята попытка ответить на эти вопросы для разнообразных ситуаций, с которыми мы столкнемся в последующих главах. Начнем, по-видимому, с простейшего случая, когда источник имеет только два возможных состояния и число наблюдаемых фиксировано.

---

¹) Множество наблюдаемых Y часто называются *статистикой;* термин «статистика» обычно относится к любому отображению одного пространства наблюдаемых [в данном случае пространства исходного процесса $y(t)$] на другое (в данном случае на пространство наблюденных координат Y). Статистика называется *достаточной,* если при этом отображении не теряется никакая информация, имеющая значение для потребителя. (*Прим. авт.*)

2.2. Выбор между двумя простыми гипотезами

Предположим, что имеется множество наблюдаемых $Y=\{y_1, y_2, \ldots, y_M\}$. Задача состоит в том, чтобы определить по этим наблюдаемым, какая из следующих двух гипотез имеет место: *нулевая гипотеза* H_0 о том, что источник находится в *нулевом состоянии* и наблюдаемые описываются условной плотностью распределения $p(Y|H_0)$, или *альтернативная гипотеза* H_1 о том, что источник находится в *альтернативном состоянии* и наблюдаемые описываются плотностью распределения $p(Y|H_1)$. Так как каждая гипотеза относится только к одному состоянию источника, то она называется *простой* гипотезой. Выбор между ними иногда называется *проверкой (тестом)* гипотезы H_0 относительно альтернативной гипотезы H_1, но вопрос о том, производится ли выбор между двумя гипотезами и принятие одной из них или вместо этого проверка одной из них и принятие или отвержение ее является, очевидно, вопросом терминологии. Существуют два вида ошибок, присущих этой процедуре проверки гипотез. Говорят, что происходит *ошибка первого рода,* когда гипотеза H_0 является верной, но отвергается в результате проверки. Аналогично *ошибка второго рода* возникает, когда верна гипотеза H_1, а принимается гипотеза H_0. Вероятность ошибки первого рода называется также *уровнем значимости* теста и обозначается через α. Вероятность ошибки второго рода обозначается β. Наконец, упомянем, что вероятность $1-\beta$ называется *мощностью* теста при проверке гипотезы H_0 относительно гипотезы H_1.

Обозначим через S пространство возможных значений наблюдаемых $Y=\{y_1, y_2, \ldots, y_M\}$. Задача проверки гипотез состоит в том, чтобы разделить пространство S на две непересекающиеся области R_0 и R_1 ($R_0+R_1=S$) так, что если Y принадлежит R_0, то принимается H_0, а если Y принадлежит R_1, то принимается H_1 (отвергается H_0). Вероятности ошибок α и β можно выразить с помощью интегралов[1]), взятых по M-мерным областям R_0 и R_1:

$$1-\int_{R_1} p(Y\mid H_0)\,dY=\int_{R_0} p(Y\mid H_0)\,dY=1-\alpha;$$

$$1-\int_{R_1} p(Y\mid H_1)\,dY=\int_{R_0} p(Y\mid H_1)\,dY=\beta. \tag{2.1}$$

Для того чтобы осуществить оптимальный выбор области R_0, необходимо задать критерий оптимальности. В связи с этим припишем численное значение, или *стоимость*, каждому возможному решению. Эта стоимость представляет собой потери (или выигрыш в случае, если стоимость является отрицательной), возникающие при каком-то частном решении. Так как стоимость отдельного решения часто не ясна, то разумно, по-видимому, предположить, что стоимость ошибочного решения больше, чем стоимость правильного решения. Это предположение в действительности достаточно для того, чтобы определить оптимальное правило решения в общем виде, которое определяется здесь как правило, минимизирующее математическое ожидание стоимости решения.

---

[1]) Если наблюдаемые y_i являются дискретными случайными величинами, то интегралы могут быть заменены суммами, а плотности распределений — вероятностями. Оба этих случая могут быть, конечно, записаны в единой форме с помощью интегралов Стильтьеса. *(Прим. авт.)*

Обозначим через C_{ij} стоимость принятия гипотезы H_i в случае, когда верной является гипотеза H_j, и пусть $p(H_i)$ обозначает априорную вероятность того, что H_i является верной гипотезой. Тогда математическое ожидание стоимости некоторого частного решения

$$E\,(\text{стоимость}) = C_{00}\int\limits_{R_0} p\,(Y \mid H_0)\,P\,(H_0)\,dY +$$

$$+ C_{01}\int\limits_{R_0} p\,(Y \mid H_1)\,P\,(H_1)\,dY + C_{10}\int\limits_{R_1} p\,(Y \mid H_0)\,P\,(H_0)\,dY +$$

$$+ C_{11}\int\limits_{R_1} p\,(Y \mid H_1)\,P\,(H_1)\,dY. \tag{2.2}$$

Так как какое-то решение должно быть принято, то

$$\int\limits_{R_0} p\,(Y \mid H_i)\,dY + \int\limits_{R_1} p\,(Y \mid H_i)\,dY = 1,$$

так что

$$E\,(\text{стоимость}) = \int\limits_{R_0} [(C_{01} - C_{11})\,P\,(H_1)\,p\,(Y \mid H_1) -$$

$$- (C_{10} - C_{00})\,P\,(H_0)\,p\,(Y \mid H_0)]\,dY + C_{11}\,P\,(H_1) + C_{10}\,P\,(H_0). \tag{2.3}$$

Математическое ожидание стоимости решения, очевидно, достигает минимума при определении R_0 как области, содержащей все те точки Y, для которых подынтегральное выражение в равенстве (2.3) отрицательно. Так как по предположению величины $C_{01} - C_{11}$ и $C_{10} - C_{00}$ положительные, то оптимальная область R_0 содержит все точки Y, удовлетворяющие неравенству

$$\frac{p\,(Y \mid H_0)}{p\,(Y \mid H_1)} > \frac{(C_{01} - C_{11})\,P\,(H_1)}{(C_{10} - C_{00})\,P\,(H_0)}. \tag{2.4}$$

Если отношение плотностей вероятностей $p(Y \mid H_0)/p(Y \mid H_1)$ превышает постоянную $(C_{01} - C_{11})P(H_1)/(C_{10} - C_{00})P(H_0)$, то в соответствии с этим тестом принимается гипотеза H_0; в противном случае гипотеза отвергается. Этот тест известен под названием *байесовского теста.*

Может случиться так, что выполняется равенство $C_{01} - C_{11} = C_{10} - C_{00}$, либо предполагают, что оно верно за неимением лучшей оценки действительных стоимостей. Оптимальное решение тогда состоит в том, что следует принять гипотезу H_i, соответствующую наибольшему из выражений $p(Y|H_i)P(H_i)$. Такого типа решение по очевидным причинам называется решением по *максимуму апостериорной вероятности.* [Иногда для этого правила решения используется термин *«идеальный наблюдатель»*. Заметим, что когда $C_{01}-C_{11}=C_{10}-C_{00}$, максимизация математического ожидания стоимости эквивалентна минимизации безусловной вероятности $P_e=\alpha P(H_0)+\beta P(H_1)$ ошибочного решения.] Если в добавление к этому априорные вероятности $P(H_i)$ равны (или предполагаются равными), $P(H_0)=P(H_1)$, то решение основывается только на использовании функций $p(Y|H_i)$, иногда называемых *функциями правдоподобия.* Решение, состоящее в принятии гипотезы H_i, для которой функция правдоподобия $p(Y|H_i)$ принимает максимальное значение, обычно называется решением по *максимуму правдоподобия.*

Если невозможно приписать стоимости различным решениям, то иногда более приемлемым является критерий *Неймана—Пирсона.* Согласно этому критерию вероятность ошибочно отвергнуть гипотезу α заранее фиксируется и используется тест, который имеет максимальную мощность $1-\beta$ среди всех тестов, имеющих уровень значимости α. Независимо от значения α оптимальным по этому критерию оказывается тест, использующий отношение плотностей вероятностей. Для того чтобы минимизировать β при фиксированном α, введем множитель Лагранжа λ и найдем такую область R_0, для которой выражение

$$\lambda\alpha+\beta=\lambda\left[1-\int\limits_{R_0}p(Y\,|\,H_0)\,dY\right]+\int\limits_{R_0}p(Y\,|\,H_1)\,dY$$

принимает максимальное значение. Но это выражение совпадает с выражением (2.3) при $P(H_0)=P(H_1)=1/2$; $C_{10}=2\lambda$; $C_{01}=2$ и $C_{11}=C_{00}=0$. Так как значения $C_{01}-C_{11}$ и $C_{10}-C_{00}$ положительны при любом положительном λ, то выполняются условия, необходимые для оптимальности выраженного неравенством (2.4) теста, использующего отношение плотностей вероятностей. Оптимальный тест, соответствующий критерию Неймана—Пирсона, приводит, следовательно, к принятию гипотезы H_0, если

$$\frac{p(Y\,|\,H_0)}{p(Y\,|\,H_1)}>\frac{1}{\lambda}, \tag{2.5}$$

и отвержению этой гипотезы в других случаях. Параметр λ определяется, очевидно, из условия $\alpha=1-\int\limits_{R}p(Y|H_0)dY$, где R состоит из всех тех множеств Y, которые удовлетворяют неравенству (2.5).

Наконец, если стоимостные функции известны, но нет разумного способа определить априорные вероятности, то можно отдать предпочтение правилу решения, которое минимизирует стоимость решения для наиболее неблагоприятного выбора этих вероятностей. Так как математическое ожидание стоимости решения является линейной функцией вероятности $P(H_0)=1-P(H_1)$, то максимум стоимости получается либо, когда $P(H_0)=1$, либо когда $P(H_1)=1$. Таким образом, эквивалентным правилом является то, для которого максимум математического ожидания стоимостей решения в случаях, когда $P(H_0)=1$ и $P(H_1)=1$, минимален. Решение, построенное в соответствии с этим правилом, называется *минимаксным решением.* Из равенства (2.3) получаем:

$$E(\text{стоимость} \mid P(H_0)=1) = C_{10} - \int\limits_{R_0} (C_{10} - C_{00})\, p(Y \mid H_0)\, dY;$$

$$E(\text{стоимость} \mid P(H_1)=1) = C_{11} + \int\limits_{R_0} (C_{01} - C_{11})\, p(Y \mid H_1)\, dY.$$

Если бы выражение для $E(\text{стоимость} \mid P(H_0)=1)$ было наибольшим из двух приведенных, то максимум математического ожидания стоимости мог бы быть уменьшен увеличением области R_0; если бы наибольшим было выражение для E $(\text{стоимость} \mid P(H_1)=1)$, то максимум мог бы быть уменьшен уменьшением области R_0. Оптимальная область R_0, следовательно, должна быть одной из таких областей R, для которой

$$\begin{aligned}
&E(\text{стоимость} \mid P(H_0)=1) = E(\text{стоимость} \mid P(H_1)=1) = \\
&= \gamma E(\text{стоимость} \mid P(H_0)=1) + (1-\gamma) E(\text{стоимость} \mid P(H_1)=1) = \\
&= \int\limits_{R_0} [(C_{01} - C_{11})\, p(Y \mid H_1)(1-\gamma) - (C_{10} - C_{00})\, p(Y \mid H_0)\gamma]\, dY + \\
&+ \gamma C_{10} + (1-\gamma) C_{11},
\end{aligned} \tag{2.6}$$

где γ — произвольная постоянная. Так как это последнее выражение совпадает по форме с выражением в (2.3), то максимум математического ожидания стоимости минимизируется при выборе области R_0, для которой

$$\frac{p(Y \mid H_0)}{p(Y \mid H_1)} > \frac{(C_{01} - C_{11})(1-\gamma)}{(C_{10} - C_{00})\gamma}, \tag{2.7}$$

где γ выбирается так, чтобы удовлетворялось первое из равенств (2.6).

Важно то, что эти решения, независимо от того, какое из правил рассматривается, основаны на сравнении отношения плотностей вероятностей $p(Y|H_0)/p(Y|H_1)$ с некоторой заранее заданной постоянной. Это отношение принято называть *отношением правдоподобия,* а тест, основанный на этом отношении, — *тестом отношения плотностей вероятностей.* Оптимальная проверка гипотез при любом из указанных выше определений оптимальности является тестом отношения плотностей вероятностей.

В следующем параграфе вновь рассматривается выбор между двумя простыми гипотезами, но для случая, когда число M наблюдаемых заранее не фиксировано.

П58391

Техническая библиотека
Киевский
авиационный завод

2.3. Последовательный тест отношения плотностей вероятностей

Тест, рассмотренный в предыдущем параграфе, основан на сравнении отношения $p(Y|H_0)/p(Y|H_1)$ с некоторой заранее определенной постоянной C. Решение принимается после того, как становятся известными все M наблюдаемых из множества Y. Но если M достаточно велико, чтобы гарантировать надежное решение почти для каждого случая, то, по-видимому, иногда правильное решение становится очевидным задолго до того, как станут известны все M наблюдаемых. Например, пусть $Y(n)$ будет множеством, состоящим из первых n наблюдаемых, и предположим, что отношение $p(Y(n)|H_0)/p(Y(n)|H_1)$ значительно больше (или значительно меньше), чем константа решения C для некоторого $n<M$. В этом случае представляется разумным и безопасным принять (или отвергнуть) нулевую гипотезу даже тогда, когда для вынесения решения используются меньше, чем M наблюдаемых. Допуская такую гибкость, найдем, что математическое ожидание числа наблюдений, необходимых для решения, может быть значительно уменьшено без увеличения вероятности вынесения неправильного решения.

Последовательный тест отношения плотностей вероятностей строится так, чтобы решение принималось в тот момент, когда это впервые можно сделать с достаточной гарантией его верности. Процедура состоит в следующем. Пусть $Y(m)$ обозначает множество наблюдаемых $\{y_1, y_2, \ldots, y_m\}$. Для каждого m определяется отношение

$$\lambda(m) = \frac{p(Y(m)|H_0)}{p(Y(m)|H_1)}. \tag{2.8}$$

Если $\lambda(m)$ больше, чем некоторое пороговое значение A, то тест завершается принятием гипотезы H_0. Если $\lambda(m)$ меньше, чем второе пороговое значение B, то H_0 отвергается. Наконец, если $B<\lambda(m)<A$, то проводятся дополнительные наблюдения, вычисляется и снова сравнивается с A и B отношение $\lambda(m+1)$. Таким образом, тест заканчивается при наименьшем значении $m=M$, для которого $\lambda(M)\geqslant A$, или $\lambda(M)\leqslant B$. Множества наблюдаемых $Y(m)$ в среднем могут быть, по-видимому, меньшими, чем те, которые необходимы для теста с фиксированным объемом выборок. Теперь, однако, число наблюдаемых, использованных в данном тесте, является случайной величиной.

Ясно, что вероятности α и β — функции пороговых значений A и B. Чтобы найти вид этой зависимости, предположим сначала, что тест закончился принятием гипотезы H_0. Пусть $Y(M)=\{y_1, y_2, \ldots, y_M\}$ представляет собой некоторое частное множество, удовлетворяющее всем неравенствам $B<\lambda(m)<A$, $m=1$,

2,..., $M-1$, $\lambda(M)\geqslant A$, и пусть R_M обозначает пространство таких множеств $Y(M)$. Тогда [1])

$$1-\alpha=\sum_{M=1}^{\infty}\int_{R_M}p(Y(M)\,|\,H_0)\,dY(M)\geqslant$$

$$\geqslant A\sum_{M=1}^{\infty}\int_{R_M}p(Y(M)\,|\,H_1)\,dY(M)=A\beta. \tag{2.9}$$

Аналогично обозначая через S_M пространство множеств $Y(M)$, приводящих после M наблюдений к отказу от гипотезы H_0, получаем

$$\alpha=\sum_{M=1}^{\infty}\int_{S_M}p(Y(M)\,|\,H_0)\,dY(M)\leqslant$$

$$\leqslant B\sum_{M=1}^{\infty}\int_{S_M}p(Y(M)\,|\,H_1)\,dY(M)=B(1-\beta). \tag{2.10}$$

Таким образом, $A\leqslant(1-\alpha)/\beta$ и $B\geqslant\alpha/(1-\beta)$.

Здесь используются знаки неравенств из-за того, что отношение $\lambda(m)$ может превысить A или быть меньше, чем B, в момент принятия или отказа от гипотезы. Но если наблюдаемые таковы, что $\lambda(m)$ не меняется быстро с изменением m, то, так как $B<\lambda(M-1)<A$, отношение $\lambda(M)$ не может сильно отличаться от A или B. Очевидно, при замене B на $\alpha/(1-\beta)$ и A на $(1-\alpha)/\beta$ длина теста может увеличиться. Тем не менее при только что описанных условиях это увеличение будет незначительным. Замена B на $\alpha/(1-\beta)$ и A на $(1-\alpha)/\beta$ изменит также вероятности ошибок. Однако, обозначая через α' и β' действительные вероятности ошибок первого и второго рода соответственно, когда A и B аппроксимируются таким образом, из равенств (2.9) и (2.10) находим, что $(1-\alpha')/\beta'\geqslant A=(1-\alpha)/\beta$ и $\alpha'/(1-\beta')\leqslant B=\alpha/(1-\beta)$. Следовательно, $\beta'\leqslant\beta'/(1-\alpha')\leqslant\beta/(1-\alpha)$, $\alpha'\leqslant\alpha'/(1-\beta')\leqslant\alpha/(1-\beta)$ и $\alpha'+\beta'\leqslant\alpha+\beta$.

Так как α и β в общем случае очень малы, возможное увеличение вероятностей ошибок из-за использования этих аппроксимаций для A и B незначительно. В некоторых случаях представляет интерес последовательный тест с $\beta\to0$. При этом $\beta'\to0$ и $\alpha'\leqslant\alpha$ независимо от значения α. Аналогичное утверждение справедливо и при $\alpha\to0$.

Оптимальный тест с фиксированным объемом выборки состоял в сравнении отношения плотностей вероятностей с пороговым значением, определяемым различными стоимостными функциями и априорными вероятностями. Вероятности ошибок α и β, в свою очередь, также определялись этим пороговым значением. Как отмечалось в начале параграфа, если рассматриваемое отношение плотностей вероятностей либо значительно больше, либо значительно меньше, чем пороговое значение, еще до того, как собраны все наблюдаемые, то представляется довольно безопасным оборвать тест в этой точке. Затем были определены *два* пороговых значения A и B и было разрешено закончить тест, когда отношение плотностей вероятностей достигнет одного из них. Вероятности ошибок α и β вновь могли быть выражены через пороговые значения. Однако в этом рассуждении не рассматривался вопрос о стоимостях. При использовании последовательного теста появляется новая стоимость, которая не учитывалась тестом с фиксированным объемом, а именно, стоимость продолжения наблюдения. В тесте с фиксированным объемом выборки стоимость наблюдения не зависела от принятого решения. Здесь же, так как длина теста зависит от вероятностей различных решений, стоимость наблюдения является функцией самого теста. Математическое ожидание стоимости последовательного теста можно записать в виде [ср. с равенством (2.3)]

---

[1]) Для простоты здесь предполагается, что тест заканчивается с вероятностью, равной единице, для некоторого значения M. Это утверждение справедливо, когда наблюдаемые статистически независимы, но его можно доказать и при более общих условиях. *(Прим. авт.)*

$$E(\text{стоимость}) = [\beta C_{01} + (1-\beta) C_{11}] P(H_1) + [\alpha C_{10} + (1-\alpha) C_{00}] P(H_0) + \\ + C_0 E(M \mid H_0) P(H_0) + C_0 E(M \mid H_1) P(H_1), \tag{2.11}$$

где C_0 — стоимость наблюдения, а $E(M|H_0)$ и $E(M|H_1)$ — условные математические ожидания длины теста при условии, что верными гипотезами были H_0 и H_1 соответственно. Можно показать, что независимо от конкретных значений этих стоимостных коэффициентов (в предположении, конечно, что все величины C_0, $C_{01}-C_{11}$ и $C_{10}-C_{00}$ положительны) существует последовательный тест отношения плотностей вероятностей, который минимизирует математическое ожидание стоимости решения. Более того, используя этот факт, можно доказать, что среди всех тестов, приводящих к некоторому заданному множеству вероятностей α и β, математическое ожидание числа наблюдаемых M, необходимых для решения при любой гипотезе, минимизируется при использовании последовательного теста отношения плотностей вероятностей. Эти доказательства, однако, довольно длинны, и подробности читатель может найти в литературе.

Эффективность последовательного теста отношения плотностей вероятностей в сравнении с другими тестами, имеющими те же самые вероятности ошибочных решений, может быть измерена с помощью математического ожидания числа M наблюдений, требуемых для выполнения теста. Вывод общего выражения для этого параметра не представляется возможным, однако оно может быть найдено в важном частном случае, когда наблюдаемые y_i являются одинаково распределенными, статистически независимыми случайными величинами и когда можно пренебречь «перескоками границ» [$\lambda(M)-A$, когда принимается H_0 и $B-\lambda(M)$, когда она отвергается]. В частности, можно показать[1]), что если $z_i \triangleq \log[p_0(y_i)/p_1(y_i)]$, где $p_j(y_i) \triangleq p(y_i|H_j)$, и если $E(z|H_0) \triangleq \triangleq E(z_i|H_0) \neq 0$, то

$$E(M|H_0) = \frac{(1-\alpha)\log A + \alpha \log B}{E(z|H_0)} =$$

$$= \frac{(1-\alpha)\log\left(\frac{1-\alpha}{\beta}\right) + \alpha \log\left(\frac{\alpha}{1-\beta}\right)}{E(z|H_0)}. \tag{2.12}$$

Подобно этому, если $E(z|H_1) \neq 0$, то

$$E(M|H_1) = \frac{\beta \log \frac{1-\alpha}{\beta} + (1-\beta)\log\frac{\alpha}{1-\beta}}{E(z|H_1)}. \tag{2.13}$$

Часто полезно иметь возможность описывать тест более полно, чем с помощью только математического ожидания числа наблюдаемых, необходимых для решения. Можно показать, что, например, при определенных условиях распределение величины M является приближенно гауссовским. В любом случае распределение M может быть, по крайней мере, частично охарактеризовано двумя параметрами: его математическим ожиданием и дисперсией. Выражения для дисперсий M имеют вид:

$$\operatorname{var}(M|H_0) = \frac{E(M|H_0)\operatorname{var}(z|H_0)}{E^2(z|H_0)} - \frac{\alpha(1-\alpha)(\log A - \log B)^2}{E^2(z|H_0)} +$$

$$+ \frac{2\alpha(1-\alpha)}{1-\alpha-\beta}\,\frac{\log A - \log B}{E(z|H_0)}[E(M|H_0) - E(M|H_1)]; \tag{2.14}$$

$$\operatorname{var}(M|H_1) = \frac{E(M|H_1)\operatorname{var}(z|H_1)}{E^2(z|H_1)} - \frac{\beta(1-\beta)(\log A - \log B)^2}{E^2(z|H_1)} +$$

$$+ \frac{2\beta(1-\beta)}{1-\alpha-\beta}\,\frac{\log A - \log B}{E(z|H_1)}[E(M|H_0) - E(M|H_1)]. \tag{2.15}$$

Наконец, приведем без доказательства следующий результат. Если нижний порог B принимается равным нулю (а верхний порог A является конечным) и если независимые случайные величины z_i нормально распределены с математическим ожиданием $E(z) = \mu$ и дисперсией $\operatorname{var}(z) = \sigma^2$, то распределение числа наблюдаемых, необходимых для завершения теста при условии, что он завершается, является приближенно гауссовским. Среднее и дисперсия этого распределения задаются равенствами (2.12)—(2.15) соответственно. Это приближение становится все более точным с ростом $(\mu/\sigma^2)\log A$. Аналогичное утверждение справедливо, когда B конечно, а $A = \infty$. Заметим, что когда $B = 0$, то $\alpha = 0$ и в выражении для $\mathrm{var}(M|H_0)$ в равенстве (2.14) остается только первый член. Аналогично, когда $A=\infty$, то $\beta=0$ и второй и третий члены в выражении для $\mathrm{var}(M|H_1)$ исчезают.

---

[1]) Так как результаты, представляющие для нас интерес, зависят от отношений логарифмов, то логарифмы могут быть взяты по любому удобному основанию, и это никак не отразится на выводах. Однако в дальнейшем всегда будет подразумеваться натуральное основание e, если не оговорено иное. *(Прим. авт.)*

2.4. Проверка сложных гипотез

Наблюдаемые, исследованные ранее, по предположению удовлетворяли одному из двух условий: либо гипотеза H_0 была верной и наблюдаемые описывались плотностью распределения $p(Y|H_0)$, либо гипотеза H_1 была верной и наблюдаемые описывались плотностью распределения $p(Y|H_1)$. Каждая из двух гипотез соответствовала одному единственному состоянию наблюдаемых; обе они были *простыми* гипотезами. Часто, однако, источник наблюдаемого явления может находиться в одном из нескольких возможных состояний; наблюдаемые, относящиеся к состоянию θ, распределены в соответствии с плотностью вероятности $p(Y|\theta)$. В таком случае иногда достаточно разделить множество возможных состояний на два непересекающихся подмножества и определить лишь то подмножество, к которому принадлежит данное состояние источника. Нулевая гипотеза H_0 состоит в том, что состояние источника θ является элементом из подмножества Ω_0, в то время как альтернативная гипотеза H_1 состоит в том, что θ принадлежит подмножеству Ω_1, причем $\Omega_0+\Omega_1$ содержит все множество возможных состояний. Каждая из этих гипотез называется *сложной* гипотезой, если соответствующее подмножество содержит более чем одно значение параметра, обозначающего состояние.

Задача проверки двух сложных гипотез возникает в целом ряде ситуаций. Можно, например, интересоваться только тем, попадет или нет θ в некоторое подмножество, а не тем, что θ примет какое-то частное значение, или θ может быть вектором $\boldsymbol{\theta}=(\boldsymbol{\Phi}_1, \boldsymbol{\Phi}_2, \ldots)$, где параметром, представляющим интерес, является только Φ_1. Если Φ_1 может принимать только два значения, то, очевидно, проверка является проверкой двух гипотез, но из-за наличия других неизвестных параметров обе гипотезы являются сложными.

В любом случае мы должны заново рассмотреть как тест с фиксированным объемом выборки, так и последовательный тест для того, чтобы понять, как они изменяются, когда гипотезы становятся сложными.

Проверка сложных гипотез при фиксированном объеме выборки. Пусть $C_0(\theta)$ и $C_1(\theta)$ стоимости, относящиеся к гипотезам H_0 и H_1 соответственно при условии, что источник находится в состоянии θ, и пусть $\pi(\theta)$ — априорная плотность распределения вероятности параметра θ, описывающего состояние. Пусть далее R_0 обозначает область принятия гипотезы H_0 и $P(\theta)$ — вероятность принять H_0 при заданном состоянии θ, т. е.

$$P(\theta)=\int_{R_0} p(Y|\theta)\,dY \overset{\Delta}{=} \begin{cases} 1-\alpha(\theta), & \theta\in\Omega_0; \\ \beta(\theta), & \theta\in\Omega_1. \end{cases}$$

Тогда математическое ожидание стоимости решения

$$E(\text{стоимость}) = \int\limits_{\theta\in\Omega_0} \pi(\theta)\,[C_0(\theta)\,(1-\alpha(\theta)) + C_1(\theta)\,\alpha(\theta)]\,d\theta +$$

$$+ \int\limits_{\theta\in\Omega_1} \pi(\theta)\,[C_0(\theta)\,\beta(\theta) + C_1(\theta)\,(1-\beta(\theta))]\,d\theta = K +$$

$$+ \int\limits_{\theta\in\Omega_0} \pi(\theta)\,(C_1(\theta) - C_0(\theta))\,\alpha(\theta)\,d\theta +$$

$$+ \int\limits_{\theta\in\Omega_1} \pi(\theta)\,(C_0(\theta) - C_1(\theta))\,\beta(\theta)\,d\theta. \tag{2.16}$$

Здесь K — постоянная, не зависящая от правила решения. Определим $\lambda_0 w_0(\theta) \triangleq (C_1(\theta) - C_0(\theta))\,\pi(\theta)$ и $\lambda_1 w_1(\theta) \triangleq (C_0(\theta) - C_1(\theta))\,\pi(\theta)$, где

$$\int\limits_{\theta\in\Omega_0} w_0(\theta)\,d\theta = \int\limits_{\theta\in\Omega_1} w_1(\theta)\,d\theta = 1.$$

Теперь, если λ_0 и λ_1 положительны (это аналог условий $C_{01} > C_{11}$ и $C_{10} > C_{00}$ в § 2.2), то оптимальное правило решения состоит в выборе такой области принятия гипотезы, которая минимизирует величину

$$\int\limits_{\theta\in\Omega_1} w_1(\theta)\,\beta(\theta)\,d\theta + \lambda \int\limits_{\theta\in\Omega_0} w_0(\theta)\,\alpha(\theta)\,d\theta, \tag{2.17}$$

где $\lambda = \lambda_0/\lambda_1$. Определим теперь H'_0 и H'_1 так, чтобы

$$p(Y \mid H'_0) = \int\limits_{\theta\in\Omega_0} p(Y \mid \theta)\,w_0(\theta)\,d\theta; \tag{2.18}$$

$$p(Y \mid H'_1) = \int\limits_{\theta\in\Omega_1} p(Y \mid \theta)\,w_1(\theta)\,d\theta. \tag{2.19}$$

Если бы R_0 была областью принятия (и $\overline{R}_0$ — областью отвержения) как простой гипотезы H'_0, так и сложной гипотезы H_0, то

$$\alpha \triangleq \int\limits_{\overline{R}_0} p(Y \mid H'_0)\,dY = \int\limits_{\overline{R}_0} \int\limits_{\theta\in\Omega_0} p(Y \mid \theta)\,w_0(\theta)\,d\theta\,dY = \int\limits_{\theta\in\Omega_0} w_0(\theta)\,\alpha(\theta)\,d\theta; \tag{2.20}$$

$$\beta \triangleq \int\limits_{R_0} p(Y \mid H'_1)\,dY = \int\limits_{\theta\in\Omega_1} w_1(\theta)\,\beta(\theta)\,d\theta. \tag{2.21}$$

Область R_0, которая минимизирует величину $\beta + \lambda\alpha$, определяется (в соответствии с обсуждавшимся ранее критерием Неймана—Пирсона), неравенством

$$p(Y \mid H'_0)/p(Y \mid H'_1) < 1/\lambda. \tag{2.22}$$

Таким образом, область принятия гипотезы H_0, определенная соотношением (2.22), также минимизирует математическое ожидание стоимости решения при сложной гипотезе [см. ф-лу (2.17)]. Если

$$C_1(\theta) - C_0(\theta) = \begin{cases} C_0, & \theta \in \Omega_0; \\ -C_1, & \theta \in \Omega_1, \end{cases}$$

где C_0 и C_1 положительные постоянные, то этот тест приводит к принятию H_0 только тогда, когда

$$\frac{\int\limits_{\theta \in \Omega_0} p(Y \mid \theta)\, \pi(\theta)\, d\theta}{\int\limits_{\theta \in \Omega_1} p(Y \mid \theta)\, \pi(\theta)\, d\theta} > \frac{C_1}{C_0}. \tag{2.23}$$

Иногда этот тест называется тестом *среднего максимального правдоподобия.*

Если функции $C_i(\theta)$ или априорная плотность вероятности $\pi(\theta)$, или и то и другое неизвестны, то функции $w_i(\theta)$ не определены. Тем не менее они часто могут быть определены разумным способом с помощью некоторого другого критерия. Взвешенная средняя вероятность ошибки $\int\limits_{\theta \in \Omega_0} \alpha(\theta)\, w_0(\theta)\, d\theta + \int\limits_{\theta \in \Omega_1} \beta(\theta)\, w_1(\theta)\, d\theta$ по-прежнему остается минимальной для теста (2.22) независимо от критерия, с помощью которого определяются весовые функции. Один из возможных способов выбора весовых функций при отсутствии достаточной априорной информации или информации о стоимости состоит в том, что полагают $w_0(\theta) = \delta(\theta - \theta')$ и $w_1(\theta) = \delta(\theta - \theta'')$, где $\delta(x)$ — дельта-функция Дирака; θ' принадлежит Ω_0, а θ'' принадлежит Ω_1. В некоторых важных случаях область принятия гипотезы, определенная неравенством (2.22), с выбранными таким образом функциями $w_0(\theta)$ и $w_1(\theta)$ может быть сделана независимой как от θ', так и от θ'' для некоторого $\lambda = \lambda(\theta', \theta'')$. Получающийся в результате тест, который называется *равномерно наиболее мощным тестом* с уровнем значимости $\alpha(\theta)$, является особенно привлекательным в этом случае, по крайней мере, если $\alpha_0 = \max\limits_{\theta \in \Omega_0} \alpha(\theta)$ и $\beta_0 = \max\limits_{\theta \in \Omega_1} \beta(\theta)$ достаточно малы. Термин «равномерно наиболее мощный тест» означает, что для любых θ_0 из Ω_0 и θ_1 из Ω_1 среди всех тестов с уровнем значимости $\alpha(\theta_0)$ этот тест имеет максимальную мощность $1 - \beta(\theta_1)$.

Могут быть определены также другие разумные тесты, отличные от теста (2.22). Один из них, тест по *максимуму правдоподобия,* состоит в определении максимума плотностей $p(Y \mid \theta)$. Если этот максимум достигается для $\theta \in \Omega_0$, то принимается гипотеза H_0;

в противном случае H_0 отвергается[1]). Тот же самый тест в более общей форме мог бы состоять в сравнении отношения

$$\frac{\max\limits_{\theta\in\Omega_0} p(Y\mid\theta)}{\max\limits_{\theta\in\Omega_1} p(Y\mid\theta)} \tag{2.24}$$

с пороговым значением C и принятии H_0 тогда и только тогда, когда пороговое значение превышено.

Последовательные тесты для сложных гипотез. Как только что было указано, области принятия гипотез при рассмотрении сложных гипотез H_0 и H_1 часто могут быть определены тестом отношения плотностей вероятностей. Если можно задать разумный тест такого вида, то следующий очевидный шаг должен состоять в исследовании последовательной процедуры решения. Однако, если отношение плотностей определено с помощью взвешенного среднего значения функций $p(Y|\theta)$, как в ф-лах (2.18) и (2.19), то последовательные наблюдаемые y_i часто не будут независимыми при любой из этих гипотез. То есть даже при $p(Y|\theta) = \prod\limits_i p(y_i|\theta)$ величина

$$\int\limits_{\theta\in\Omega_\nu} p(Y\mid\theta)\,w_\nu(\theta)\,d\theta = \int\limits_{\theta\in\Omega_\nu} \prod_i p(y_i\mid\theta)\,w_\nu(\theta)\,d\theta$$

в общем случае не равна $\prod\limits_i \int\limits_{\theta\in\Omega_\nu} p(y_i|\theta)\,w_\nu(\theta)\,d\theta$ как для $\nu=0$, так и для $\nu=1$. Тем не менее в рассуждениях, приводящих к ф-лам (2.9) и (2.10), использовалось предположение о независимости наблюдаемых y_i только для доказательства того, что тест в конце концов заканчивается. Это свойство можно доказать и при значительно более общих условиях. При условии, что оно имеет место, соотношения (2.9) и (2.10) справедливы также в случае тестов для сложных гипотез. Если верхний порог A равен $(1-\alpha)/\beta$, а нижний порог B равен $\alpha/(1-\beta)$, то равенства (2.20), (2.21) также будут удовлетворяться для последовательного теста. Здесь применимы те же замечания, касающиеся выбора весовых функций, что и в случае теста с фиксированным объемом выборки.

При выводе выражений (см. § 2.3) для среднего и дисперсии числа наблюдаемых, необходимых для решения при использовании последовательного теста, довольно существенно используется предположение о независимости наблюдаемых. В общем случае, при отсутствии независимости, трудно получить сравнимые результаты. Однако наблюдаемые y_i остаются независимыми для некоторых специальных классов весовых функций, таких, как $w_\nu(\theta) = \delta(\theta-\theta_\nu)$. В более общем случае, если θ является вектором $\theta = (\theta_1, \Phi_1, \Phi_2, \ldots, \Phi_k)$, если

---

[1]) Заметим, что это определение теста по максимуму правдоподобия эквивалентно приведенному в § 2.2 для случая, когда H_0 и H_1 были простые гипотезы. *(Прим. авт.)*

$w_\nu(\theta) = \delta(\theta - \theta_\nu) f_1(\Phi_1) f_2(\Phi_2) \dots f_k(\Phi_k)$ и $p(Y \mid \theta) = \prod_i p(y_i \mid \theta, \Phi_i)$, то

$$\int p(Y \mid \theta) w_\nu(\theta)\, d\theta = \int \dots \int \prod_i p(y_i \mid \theta_\nu, \Phi_i) f_i(\Phi_i)\, d\Phi_1 \dots d\Phi_k =$$

$$= \prod_i \int p(y_i \mid \theta_\nu, \Phi_i) f_i(\Phi_i)\, d\Phi_i = \prod_i p(y_i \mid \theta_\nu)$$

и наблюдаемые статистически независимы. Тест эквивалентен различению двух простых гипотез.

Вероятность $P(\theta)$ того, что последовательный тест отношения плотностей вероятностей заканчивается принятием нулевой гипотезы H_0, когда источник находится в состоянии θ в предположении, что наблюдаемые независимы и одинаково распределены, равна

$$P(\theta) = \frac{1 - B^{h(\theta)}}{A^{h(\theta)} - B^{h(\theta)}}, \tag{2.25}$$

где $h(\theta)$ — единственное ненулевое решение уравнения

$$\Phi(h) = E\left(e^{hz} \mid \theta\right) = 1 \quad \left(z = \log_e \frac{p_0(y)}{p_1(y)}\right).$$

Математическое ожидание числа наблюдаемых, необходимых для решения при этих же условиях, равно

$$E(M \mid \theta) = \frac{P(\theta) \log A + (1 - P(\theta)) \log B}{E(z \mid \theta)}. \tag{2.26}$$

Заметим, что если θ_0 предполагается состоянием, соответствующим нулевой гипотезе, то $h(\theta_0) = -1$ является решением уравнения $\Phi(h) = 1$ и вследствие того, что это уравнение имеет только одно ненулевое решение, имеем $P(\theta_0) = A(1-B)/(A-B) = 1-\alpha$. Если θ_1 является состоянием, соответствующим альтернативной гипотезе, то $h(\theta_1) = 1$ и $P(\theta_1) = (1-B)/(A-B) = \beta$. Так как $A > 1$ и $B < 1$, то, если α и β будут положительными, вероятность $P(\theta)$ является монотонно убывающей функцией $h(\theta)$. Таким образом, если неравенство $h(\theta) \geqslant h(\theta_1) = 1$ удовлетворяется для всех θ из Ω_1, то максимум вероятности принятия гипотезы H_0 будет равен β и будет иметь место, когда θ_1 является в действительности наблюдаемым состоянием. Подобно этому, если $h(\theta) < -1$, то нулевая гипотеза будет принята с вероятностью большей, чем $1-\alpha$.

2.5. Поиск

В предыдущих параграфах задача состояла в том, чтобы определить, к какому из двух возможных подмножеств Ω_0 или Ω_1 принадлежит состояние θ. Предположим, однако, что требуется бо́льшая информация относительно θ; в частности, предположим, что множество состояний Ω разбито на N подмножеств $\omega_1, \omega_2, \dots, \omega_N$ и что задача состоит в том, чтобы определить подмножество ω_i, наилучшим образом характеризующее состояние источника θ. Если $N>2$, то тест называется *проверкой многих гипотез.* Если ω_i представляет собой только одно возможное состояние θ, то соответствующая гипотеза H_i — простая; в противном случае она является сложной. В любом случае проверка многих гипотез может оказаться в вычислительном отношении значительно более сложной по сравнению с проверкой двух гипотез. В действительности практические соображения могут исключить возможность проведения такого теста. Если это так, то может возникнуть необходимость, во-первых, сгруппировать гипотезы ω_i в два подмножества, скажем, Ω_1 и $\overline{\Omega}_1$, причем $\Omega_1+\overline{\Omega}_1$ содержит объединение подмножеств ω_i. В этом случае тест будет состоять в выборе множества наблюдаемых Y_1 и решении, следует ли принять нулевую гипотезу H_1 (θ принадлежит подмножеству Ω_1) или альтернативную гипотезу $\overline{H}_1$ (θ принадлежит $\overline{\Omega}_1$). Такое решение уменьшает число конкурирующих гипотез, оставляя гипотезы, принадлежащие либо подмножеству Ω_1, либо подмножеству $\overline{\Omega}_1$. Если затем разделить эти остающиеся гипотезы на два новых подмножества Ω_2 и $\overline{\Omega}_2$, представляющих две гипотезы H_2 и $\overline{H}_2$, то второй тест по проверке двух гипотез, основанный на использовании множества наблюдаемых Y_2, снова уменьшает число рассматриваемых гипотез. Если продолжить эту процедуру, выбирая надлежащим образом последовательные гипотезы H_1, H_2, H_3, ..., то, в конце концов, останется только одна из конкурировавших гипотез. Будем называть этот процесс сведения проверки многих гипотез к последовательности проверок двух гипотез *поиском.*

Целью поиска является уменьшение сложности проверки многих гипотез, возможно, за счет увеличения времени, необходимого для решения. Хотя конечная цель состоит в указании определенного подмножества ω_i состояний источника, эта цель будет достигаться с помощью получения ответов на последовательность более простых, как мы надеемся, вопросов. Этот подход является типичным, например, когда состоянием источника является его положение в пространстве или во времени. Часто более эффективной процедурой является такая, когда не спрашивают: «Где он находится?», а «Находится ли он здесь?».

Если желательно существенно уменьшить сложность вычислений с помощью процедуры поиска, то гипотезы H_i и $\overline{H}_i$ должны быть такими, чтобы возникающие в результате тесты были намного проще, чем первоначальная проверка многих гипотез. Так как H_i и $\overline{H}_i$ по всей вероятности будут сложными, если используется только что описанная процедура, то часто на практике необходимы дальнейшие упрощения. По этой причине здесь и в следующем параграфе рассмотрены лишь такие ситуации, в которых каждое подмножество ω_i характеризует одно единственное состояние источника θ_i. На j-м шаге поиска будет проверяться гипотеза H_j: $\theta=\theta_i$ (с $i=j$ по модулю N) по отношению к некоторой альтернативной (предположительно простой) гипотезе $\overline{H}_j$ (будем называть это проверкой состояния θ_i). Проверка заканчивается тогда, когда выносится решение, что некоторое состояние является верным. Будем также рассматривать разновидность этой стратегии, в которой поиск прекращается после того, как все N состояний проверены по одному разу. Если к этому моменту ни одно состояние не было объявлено верным, то может быть использован некоторый другой критерий решения; например, может быть выбрано состояние, соответствующее наибольшему значению отношения правдоподобия. Другие разновидности встречаются в задачах в конце этой главы и в последующих главах.

Вначале определим вероятность того, что поиск является успешным в случае, когда разрешается продолжать его бесконечно и когда на каждом этапе поиска вероятность α неправильного отвержения не зависит от состояния источника, а вероятность неправильного принятия ее не зависит от состояния, которое проверяется. (Эти ограничения впоследствии будут ослаблены.) Пусть $P(\mu)=1/N$ обозначает априорную вероятность того, что источник находится в μ-м состоянии. Тогда вероятность того, что состояние источника определено правильно,

$$P_c = \sum_{\mu=0}^{N-1} \sum_{j=0}^{\infty} P(\mu)(1-\beta)^{j(N-1)+\mu} \alpha^j (1-\alpha) = \frac{(1-\alpha)\left[1-(1-\beta)^N\right]}{N\beta\left[1-\alpha(1-\beta)^{N-1}\right]}. \tag{2.27}$$

Этот результат приводит к упрощенной формуле, которая будет полезна в дальнейшем. А именно, если вероятность ошибки мала, то должно выполняться неравенство

$$N\beta \ll 1-\alpha \quad (P_e \ll 1). \tag{2.28}$$

Действительно, так как P_c, очевидно, является убывающей функцией α и при $\alpha=0$

$$P_c = \frac{1-(1-\beta)^N}{N\beta} = 1 - \frac{N-1}{2}\beta + \frac{(N-1)(N-2)}{6}\beta^2 + \dots,$$

то вероятность ошибки $P_e=1-P_c$ мала по сравнению с единицей, только если $N\beta \ll 1$. Но если $N\beta \ll 1$, то равенство (2.27) можно упростить, сохранив только главные члены в разложении в степенной ряд функций $(1-\beta)^N$ и $(1-\beta)^{N-1}$. В результате получаем соотношение

$$\frac{N-1}{2}\beta \approx \frac{(1-\alpha)P_e}{1+\alpha-2\alpha P_e} \quad (\text{для } P_e \ll 1), \tag{2.29}$$

неравенство (2.28) верно для всех $P_e \ll 1$.

Для дальнейшего заметим, что приближение (2.29) остается справедливым для любого значения $P_e<1$, если $\alpha \to 1$. Действительно, из равенства (2.27) следует, что выражение $(1-\beta)^{N-1}$ должно стремиться к единице при $\alpha \to 1$, если вероятность P_c не стремится к нулю. Таким образом, снова $N\beta \ll 1$, и это предположение является единственным, необходимым для справедливости приближения (2.29).

Вероятность того, что будут проверены $\nu = jN+i+1$ состояний до принятия окончательного решения, равна

$$\Pr(\nu = jN+i+1) = \sum_{\mu=0}^{N-1} \Pr(\nu = jN+i+1\,|\,\mu)\,P(\mu) =$$

$$= \frac{1}{N}(1-\beta)^{j(N-1)}\alpha^{j}\,[(1-\beta)^{i}(1-\alpha) +$$

$$+ i\alpha\beta(1-\beta)^{i-1} + (N-i-1)\beta(1-\beta)^{i}], \tag{2.30}$$

где

$$\Pr(\nu = jN+i+1\,|\,\mu) = \begin{cases} (1-\beta)^{j(N-1)+i}\,\alpha^{j}(1-\alpha), & i=\mu; \\ (1-\beta)^{j(N-1)+i-1}\,\alpha^{j+1}\beta, & i>\mu; \\ (1-\beta)^{j(N-1)+i}\,\alpha^{j}\beta, & i<\mu. \end{cases}$$

Следовательно, математическое ожидание числа проверенных состояний

$$E(\nu) = \sum_{\nu=0}^{\infty} \nu\Pr(\nu) = \frac{1}{N}\sum_{i=0}^{N-1}\sum_{j=0}^{\infty}(jN+i+1)\Pr(\nu = jN+i+1). \tag{2.31}$$

Хотя эта сумма легко вычисляется, получающееся в результате выражение довольно неудобно для дальнейшего использования. Однако если $P_e \ll 1$, то согласно (2.28) имеем: $N\beta \ll 1-\alpha$, и получается полезная приближенная формула

$$E(\nu) \approx N\alpha/(1-\alpha) + (N+1)/2. \tag{2.32}$$

При этом же условии ($P_e \ll 1$) находим, что

$$\operatorname{var}(\nu) \approx N^2\alpha/(1-\alpha)^2 + (N^2-1)/12. \tag{2.33}$$

Предыдущие выражения были получены в предположении, что поиск может продолжаться бесконечно. Если поиск заканчивается после исследования N-го состояния, как указывалось ранее, то математическое ожидание числа состояний, которые должны быть проверены,

$$E(\nu) = \frac{1}{N}\sum_{i=0}^{N-1}(i+1)\Pr(\nu = i+1) + N\alpha(1-\beta)^{N-1} \tag{2.34}$$

[ср. с равенством (2.31)]. Если $N\beta$ мало, то приближенно

$$E(\nu) \approx (N+1)/2 + (N-1)\alpha/2. \tag{2.35}$$

Вероятность ошибки

$$P_e = 1 - \frac{1}{N}\sum_{i=0}^{N-1}(1-\beta)^{i}(1-\alpha) =$$

$$= 1-(1-\alpha)\,\frac{1-(1-\beta)^{N}}{N\beta} \approx \alpha + \frac{N-1}{2}\beta, \tag{2.36}$$

где отказ от принятия окончательного решения после проверки всех N состояний также отнесен к ошибкам.

Если α и β зависят от рассматриваемых состояний, то полученные выше результаты все же остаются полезными при отыскании границ для параметров поиска. Приближенные выражения для среднего и дисперсии числа проверенных состояний [равенства (2.32) и (2.33)] являются монотонно возрастающими функциями α, вероятность ошибки (ф-ла (2.27)) — возрастающей функцией как α, так и β. Таким образом, верхнюю и нижнюю границы для этих величин легко установить, используя верхнюю и нижнюю границы для α и β.

Если на каждом этапе поиска проводятся тесты с фиксированными объемами выборок и для выполнения каждого теста необходимы M наблюдаемых, то общее число M_T наблюдаемых, требуемых для поиска, точно равно математическому ожиданию числа тестов $E(\nu)$, умноженному на M. Как M_T, так и P_c — вероятность успешного завершения поиска — функции α и β. По-видимому, эти параметры могут быть согласованы так, чтобы минимизировать M_T при условии, что вероятность P_c ограничена. Это может быть сделано, однако (в случае, если заданы статистики теста), только тогда, когда известно соотношение, связывающее M с α и β. Поэтому дальнейшее обсуждение этой стороны проблемы отложим до рассмотрения более конкретных задач (см. гл. 6). Случай, когда на каждом этапе проводятся последовательные тесты, изучается более подробно в следующем параграфе.

Прежде чем закончить параграф, упомянем две разновидности приведенных выше стратегий поиска, которые не только интересны сами по себе, но также указывают на некоторые недостатки, свойственные подходу с фиксированным объемом выборки. Первая разновидность состоит в разбиении поиска на два (или более) этапа. На первом этапе производится относительно быстрый поиск; скорость достигается за счет довольно большого значения вероятности ошибочного принятия β по сравнению с той, которую хотелось бы получить в конце концов. После того как условно отобраны одно или большее число состояний, переходят ко второму этапу, когда каждое принятое состояние проверяется в течение несколько более длинного периода времени, чем тот, который требуется для принятия решения при первом рассмотрении. В конце этого испытательного периода каждое рассматриваемое состояние окончательно принимается или отвергается. Поиск заканчивается, когда либо одно состояние принято, либо когда все состояния были отвергнуты. Очевидно обобщение этой процедуры на случай, когда поиск осуществляется более чем в два этапа.

Преимущество этого подхода легко видеть. Предположим, что первый из тестов включает M_1 наблюдаемых и что вероятности ошибочного отвержения и ошибочного принятия при этом тесте соответственно равны α_1 и β_1. Пусть M_2, α_2 и β_2 являются соответствующими параметрами второго теста. Вероятность ошибочного отказа для объединенного теста $\alpha=\alpha_1+\alpha_2(1-\alpha_1)$, в то время как вероятность ошибочного принятия гипотезы $\beta=\beta_1\beta_2$. Математическое ожидание числа наблюдаемых для решения, когда проверяется правильное состояние, $M_c=M_1+(1-\alpha_1)M_2$, в то время как математическое ожидание, необходимое при проверке любого другого состояния, $M_e=M_1+\beta_1M_2$.

Так как по предположению β_1, β_2, α_1 и α_2 являются малыми, то ошибочные состояния могут быть отвергнуты с намного большей надежностью, чем это можно было бы сделать с помощью только лишь первого теста, в то время как правильное состояние отвергается лишь с немного большей вероятностью, чем ранее. Более того, если $M_2\gg M_1$, то время проверки ошибочных состояний увеличивается значительно по отношению ко времени проверки правильного состояния. Когда общее число состояний велико (и имеется только одно правильное состояние), этот метод дает значительные преимущества.

Преимущество, связанное с увеличением относительного времени проверки правильного состояния, реализуется также в другой модификации поиска с фиксированным объемом выборки. Здесь также имеется два этапа работы. На первом этапе каждое состояние опять проверяется в течение относительно короткого промежутка времени, но при этом никакое решение не выносится. Вместо этого записывается отношение правдоподобия. На втором этапе состояния исследуются в порядке убывающих значений их отношений правдоподобия, и решение о принятии или отвержении каждого состояния проводится так, как в случае, когда процесс поиска не разбит на этапы. Таким образом, сначала проверяются наиболее вероятные состояния, поэтому время проверки ошибочных состояний, по всей вероятности, будет уменьшено.

Наиболее серьезным недостатком методов поиска с фиксированным объемом выборки является неэффективное использование имеющейся в распоряжении информации. В начале поиска, когда некоторое число состояний уже отвергнуто, эффективные априорные вероятности оставшихся состояний увеличиваются. Порог, соответствующий принятию гипотезы, должен бы поэтому соответственно уменьшиться. Учет этого факта, однако, привел бы к устранению первоначального преимущества этой процедуры поиска, а именно, ее простоты. Неэффективность еще больше возрастает, если до принятия решения некоторые состояния проверяются более чем один раз. Для выяснения в i-й раз, нужно ли принять или отвергнуть состояние, используется отношение плотностей вероятностей вида $p_0(Y_{\nu i})/p_1(Y_{\nu i})$, где $Y_{\nu i}$ означает i-е множество наблюдаемых, относящихся к ν-му этапу. Это вся информация, вообще используемая на каждом этапе. Заметим, однако, что после i независимых наблюдений отношение плотностей вероятностей $\prod\limits_{j=1}^{i}[p_0(Y_{\nu j})]/[p_1(Y_{\nu j})]$ является намного лучшей мерой того, наблюдается ли ν-е состояние или нет. Так как каждый из сомножителей этого произведения должен был быть определен ранее, то особенно неэффективно использование только одного из них для принятия решения. Все это приводит к мысли об использовании какого-либо последовательного теста.

2.6. Последовательный поиск

Многие из трудностей, связанных с поиском при фиксированном объеме выборки, могут быть устранены, если для каждого исследуемого состояния можно осуществить последовательный тест. Во-первых, исчезают недостатки теста с фиксированным объемом выборки, связанные с необходимостью многократных наблюдений каждого состояния. Это происходит потому, что (в случае, когда можно пренебречь «перескоками границ») отношение плотностей вероятностей $p_0[Y_{\nu i}(M_i)]/p_1[Y_{\nu i}(M_i)]$ в конце i-го теста равно постоянной B для всех тестов, кроме последнего. Таким образом.

$$\prod_{j=1}^{i-1} \frac{p_0[Y_{\nu j}(M_j)]}{p_1[Y_{\nu j}(M_j)]} = B^{i-1},$$

где B — заданная постоянная. Так как эта величина является одной и той же для каждого отвергнутого состояния. то решения, принятые во время i-й серии тестов, не будут меняться, даже если принять ее во внимание.

Другое преимущество последовательного поиска, которое может быть существенным, основано на потенциальной возможности устранить операции проверочного типа, часто требуемые при поиске с фиксированным объемом выборки. Способность распознавать ошибочные решения для того, чтобы заново начать поиск и одновременно способность минимизировать вероятность перехода к повторному поиску, если решение является правильным, присущи последовательному поиску.

Прежде чем подробно рассмотреть эти вопросы, определим сначала математическое ожидание числа наблюдаемых M_T, необходимых для завершения последовательного поиска. Вероятность $\Pr(\nu)$ того, что будут проверены ν состояний до того, как будет вынесено решение, дается равенством (2.30) независимо от того, проводится ли последовательный тест или тест с фиксированным объемом выборки. Если распределение наблюдаемых $Y_j = \{y_i^{(j)}\}$ в тесте зависит не от того, какое состояние θ_j проверяется, а от того, является ли оно истинным состоянием источника[1]), то условные распределения $P(M|A)$ и $P(M|R)$ чисел наблюдаемых, необходимых для того, чтобы принять или отвергнуть некоторое конкретное состояние, не зависят от проверяемого состояния. Математическое ожидание величины M_T поэтому может быть выражено в виде

---

[1]) Более общий случай рассмотрен ниже. **(*Прим. авт.*)**

$$E(M_T)=\sum_{\nu=1}^{\infty}\Pr(\nu)E(M_T|\nu)=\sum_{\nu=1}^{\infty}[E(M|R)(\nu-1)+$$

$$+E(M|A)]\Pr(\nu)=E(\nu-1)E(M|R)+E(M|A), \qquad (2.37)$$

где $E(M|R)$ и $E(M|A)$ — математические ожидания числа наблюдений, необходимых, чтобы отвергнуть или принять проверяемое состояние. Аналогично дисперсия числа наблюдаемых, необходимых для решения,

$$\mathrm{var}(M_T)=E(M_T^2)-E^2(M_T)=\sum_{\nu=0}^{\infty}E(M_T^2|\nu)\Pr(\nu)-E^2(M_T).$$

Но $E(M_T^2|\nu)=E\left(\sum_{i=1}^{\nu}M_i\right)^2=(\nu-1)E(M^2|R)+$

$$+E(M^2|A)+(\nu-1)(\nu-2)E^2(M|R)+2(\nu-1)E(M|R)E(M|A),$$

так что

$$\mathrm{var}(M_T)=E(\nu-1)\,\mathrm{var}(M|R)+E^2(M|R)\,\mathrm{var}(\nu-1)+\mathrm{var}(M|A). \qquad (2.38)$$

Оба выражения $E(\nu)$ и $\mathrm{var}(\nu)$ были найдены в предыдущем параграфе. Среднее значение и дисперсия числа наблюдаемых M_T, необходимых для решения, являются функциями как α, так и β. Эти два параметра, однако, не являются независимыми, при любой заданной вероятности ошибки P_e они подчиняются равенству (2.27). Используя это равенство совместно с ф-лами (2.37) и (2.38), получаем выражения для среднего значения и дисперсии величины M_T через α (или β), вероятности ошибки P_e, числа состояний N и условных моментов (по предположению независимых) случайных величин $z_i=\log[p_0(y_i)/p_1(y_i)]$.

Так как получающиеся в результате общие выражения для $E(M_T)$ и $\mathrm{var}(M_T)$ довольно сложны, то некоторые наиболее важные частные случаи приведены в табл. 2.1. Формулы упрощаются, если использовать приближения, полученные в предыдущем параграфе [равенства (2.29), (2.32) и (2.33)]. Случай, когда обе величины α и β являются малыми, представляет интерес как для сравнения с другим крайним случаем ($\alpha\to1$), так и для последующего сравнения с методом поиска при фиксированном объеме выборки, который обычно имеет практическую ценность только при $\alpha\to1$. Так как $E(M_T)$ становится бесконечным при $\alpha\to0$, то осмысленное сравнение возможно только при $\alpha>0$. Чтобы рассмотреть этот предельный случай, мы до некоторой степени произвольно приравняем α к $P_e/2$ и β к $P_e/(N-1)$. Заметим, что если α и β определены таким образом, то справедливо равенство (2.36). Вероятность P_e, следовательно, учитывает событие, когда решение не было при-

Таблица 2.1

Условия	$E(M_T)$	$\operatorname{var}(M_T)$
Общий случай	$E(\nu-1)\,E(M\|R)+E(M\|A)$	$E(\nu-1)\operatorname{var}(M\|R)+\operatorname{var}(\nu-1)\,E^2(M\|R)+\operatorname{var}(M\|A)$
$P_e \ll 1$	$\frac{(N-1)(1+\alpha)}{2(1-\alpha)}\frac{\log\frac{1}{\alpha}}{\mu_1}-$ $-\frac{\alpha}{1-\alpha}\frac{\log\frac{1}{\alpha}}{\mu_0}+$ $+\frac{\log\left(\frac{N-1}{P_e}\frac{1+\alpha}{2}\right)}{\mu_0}$	$\left(\frac{N^2-1}{12}+\frac{N^2\alpha}{(1-\alpha)^2}\right)\frac{\log^2\frac{1}{\alpha}}{\mu_1^2}+$ $+\frac{(N-1)(1+\alpha)}{2(1-\alpha)}\frac{\sigma_1^2}{\mu_1^3}\times$ $\times\log\frac{1}{\alpha}\frac{\sigma_0^2}{\mu_0^3}\left[\log\left(\frac{N-1}{P_e}\frac{1+\alpha}{2}\right)-\frac{\alpha}{1-\alpha}\log\frac{1}{\alpha}\right]$ $-\frac{\alpha\log^2\frac{1}{\alpha}}{(1-\alpha)^2}\left(\frac{1}{\mu_0}+\frac{1}{\mu_1}\right)^2 \quad \left(P_e\ll\frac{N\mu_0}{\mu_1}\right)$
$P_e \ll 1$ $\alpha=\frac{P_e}{2}$ $\beta=\frac{P_e}{N-1}$	$\frac{N-1}{2}\frac{\log\frac{2}{P_e}}{\mu_1}+\frac{\log\frac{N-1}{P_e}}{\mu_0}$	$\frac{N^2-1}{12}\left(\frac{\log\frac{2}{P_e}}{\mu_1}\right)^2+\frac{N-1}{2}\frac{\sigma_1^2}{\mu_1^3}\log\frac{2}{P_e}+$ $+\frac{\sigma_0^2}{\mu_0^3}\log\frac{N-1}{P_e}$

$\alpha\to 1,\quad \beta\to 0$ $P_e\leqslant (N-1)/N$	$\frac{P_e}{\mu_1}(A^*-1-\log A^*)+\frac{1}{\mu_0}(1-P_e)\times$ $\times\left(\log A^*-\frac{A^*-1}{A^*}\right)$	
$\alpha\to 1,\quad \beta\to 0$ $P_e\ll 1$	$\frac{N-1}{\mu_1}+\frac{\left(\log\frac{N-1}{P_e}-1\right)}{\mu_0}$	$\frac{N^2}{\mu_1^2}+(N-1)\frac{\sigma_1^2}{\mu_1^3}+\frac{\sigma_0^2}{\mu_0^3}\left(\log\frac{N-1}{P_e}-1\right)-$ $-\left(\frac{1}{\mu_0}+\frac{1}{\mu_1}\right)^2\quad\left(P_e\ll\frac{N\mu_0}{\mu_1}\right)$
$P_e\ll 1,\quad \beta=0$ (непрерывно продолжаемый поиск)	$\left\{\frac{\alpha N}{1-\alpha}+\frac{N-1}{2}\right\}\frac{\log\frac{1}{\alpha}}{\mu_1}$	$\left(\frac{N^2-1}{12}+\frac{N^2\alpha}{(1-\alpha)^2}\right)\frac{\log^2\frac{1}{\alpha}}{\mu_1^2}+$ $+\left(\frac{N-1}{2}+\frac{\alpha N}{1-\alpha}\right)\frac{\sigma_1^2}{\mu_1^3}\log\frac{1}{\alpha}$
$\alpha=P_e\ll 1,\quad \beta=0$ (непрерывно продолжаемый поиск)	$\frac{N-1}{2}\,\frac{\log\frac{1}{P_e}}{\mu_1}$	$\frac{N^2-1}{12}\,\frac{\log^2\frac{1}{P_e}}{\mu_1^2}+\frac{N-1}{2}\,\frac{\sigma_1^2}{\mu_1^3}\log\frac{1}{P_e}$
$\alpha\to 1,\quad \beta=0$ $P_e\ll 1$ (непрерывно продолжаемый поиск)	$\frac{N}{\mu_1}$	$\frac{N^2}{\mu_1^2}+\frac{N\sigma_1^2}{\mu_1^3}$

Обозначения: $\mu_i=\lvert E(z\mid H_i)\rvert;\quad A^*=\lim\limits_{\substack{\alpha\to 1\\ \beta\to 0}}\left(\frac{1-\alpha}{\beta}\right)=\frac{(N-1)(1-P_e)}{P_e}$

$\sigma_1^2=\operatorname{var}(z\mid H_i);$

нято к моменту времени, когда каждое состояние было проверено точно один раз.

Обращаясь к табл. 2.1, можно увидеть, что в обычной ситуации, когда величины $E(z|H_0)$ и $E(z|H_1)$ имеют один и тот же порядок и $N \gg \log[(N-1)/P_e]$, время поиска для случая, когда величина α мала, приблизительно в $\frac{1}{2}\log(2/P_e)$ раз больше, чем время поиска для случая, когда $\alpha \to 1$. Аналогично дисперсия времени поиска уменьшается, грубо говоря, в $\frac{1}{12}\log^2(2/P_e)$ раз при $\alpha \to 1$.

Возможность ошибки при принятии какого-то состояния в качестве истинного состояния источника может оказаться неприятным свойством процедуры поиска, использующей схему контроля, так как схема контроля может ошибочно начать вновь весь поиск. В последовательном тесте отношения плотностей вероятностей это неудобство можно иногда устранить, если положить вероятность β равной нулю. Это предположение эквивалентно тому, что пороговое значение A становится бесконечным, и, следовательно, тому, что любое состояние никогда не будет признано правильным. Вместе с тем истинное состояние будет отвергаться с вероятностью α, а все другие состояния будут отвергаться с вероятностью 1. Следовательно, с вероятностью $1-\alpha$ аппаратура поиска будет неспособна отвергнуть истинное состояние и поэтому будет наблюдать его бесконечное число раз. Во многих приложениях истинное состояние отыскивается только с целью продолжения наблюдений. В этих случаях такой подход может оказаться вполне удовлетворительным.

Представление о никогда не завершающемся поиске равносильно признанию, что может быть получена новая информация, которая приведет к тому, что временно принятое правильным состояние будет отвергнуто. Из-за этого свойства, а также для того, чтобы отличать этот метод от более привычного, только что рассмотренного метода, будем называть описанную процедуру поиска *непрерывно продолжаемым* поиском. Вероятность правильного решения будет идентифицироваться с вероятностью того, что в некоторый момент времени истинное состояние было проверено и впоследствии никогда не будет отвергнуто.

Если формально поиск никогда не прекращается, то нужно несколько изменить определение времени поиска, чтобы оно имело смысл. Так как состояние источника эффективно определено в тот момент, когда аппаратура поиска начинает проверять состояние, которое не может быть впоследствии отвергнуто, то время поиска можно определить как время, необходимое для достижения этого момента. Это эквивалентно тому, что величины $E(M|A)$ и $\operatorname{var}(M|A)$ полагаются равными нулю в выражениях для среднего и дисперсии общего времени поиска. Получающиеся в результате выражения для $E(M_T)$ и $\operatorname{var}(M_T)$ (с $\beta=0$) также приведены в табл. 2.1.

Как и в случае поиска с фиксированным объемом выборки, полученные результаты могут быть использованы для определения границ, в которых лежат параметры поиска, даже в тех случаях, когда вероятность принятия ошибочного решения является функцией проверяемого состояния. Этот подход, однако, будучи в общем довольно удовлетворительным для процедур поиска с фиксированным объемом выборки, может приводить к довольно плохим границам для последовательного поиска. Лучшие границы можно получить, если принять во внимание, что в случае, когда альтернативная гипотеза в действительности является сложной (даже если для целей теста она заменена простой гипотезой), некоторые ошибочные состояния могут быть отклонены в среднем намного быстрее, чем другие.

В двух случаях, представляющих наибольший интерес, когда $\alpha\to 1$ и $\beta\to 0$ и когда $\alpha=P_e/2$ и $\beta=P_e/(N-1)$ (в обоих случаях $P_e\ll 1$), более точные оценки числа наблюдаемых M_T, необходимых для завершения теста, нетрудно получить даже при более общих условиях, чем только что описанные. Пусть в рассматриваемом случае $y^{(i)}$ — наблюдаемая, относящаяся к i-му состоянию, подлежащему проверке, и пусть $z^{(i)}=\log[p_0(y^{(i)})/p_1(y^{(i)})]$ — соответствующая статистика теста. Если источник находится в j-м состоянии, то пусть статистика $z^{(i)}$ характеризуется плотностью распределения $p(z^{(i)}\mid j)$ с $p(z^{(i)}\mid i)=p_0(z^{(i)})$ для всех i. Плотность распределения $p(z^{(i)}\mid j)$ может быть функцией как i, так и j, но *множество* функций $\{p(z^{(i)}\mid j),\ j=0,\ 1,\ \ldots,\ N-1\}$ по предположению будет считаться независимым от i. (Это последнее условие всегда удовлетворяется в рассматриваемых ниже применениях алгоритма последовательного поиска. В действительности $p(z^{(i)}\mid j)$ будет во всех случаях функцией лишь разности $i-j$ по модулю N.) Плотность распределения альтернативной гипотезы $p_1(y^{(i)})$ по предположению определяется так, что проверка i-го состояния оканчивается его принятием с вероятностью $1-\alpha$, если источник в действительности находится в этом состоянии, и с вероятностью *самое большее* β, если он находится в j-м состоянии для любых $j\neq i$ по модулю N.

Пусть ν обозначает число состояний, проверенных до того, как было принято решение, а M_i — число наблюдаемых, необходимых для i-го теста. Тогда

$$E(M_T)=E\left(\sum_{i=1}^{\nu} M_i\right)=\sum_{n=1}^{\infty}\left[\Pr(\nu=n)\sum_{i=1}^{n}E(M_i\mid\nu=n)\right]=$$

$$=\sum_{i=1}^{\infty}\sum_{n=i}^{\infty}\Pr(\nu=n)\,E(M_i\mid\nu=n). \qquad (2.39)$$

Замечая, что $\sum\limits_{n=i}^{\infty}\Pr(\nu=n\mid\nu\geqslant i)\,E(M_i\mid\nu=n)=E(M_i\mid\nu\geqslant i)$ и что $\Pr(\nu=n)=\Pr(\nu=n\mid\nu\geqslant i)\Pr(\nu\geqslant i)$ для всех $n\geqslant i$, получаем

$$E(M_T)=\sum_{i=1}^{\infty}\Pr(\nu\geqslant i)\,E(M_i\mid\nu\geqslant i). \qquad (2.40)$$

В общем случае случайная величина M_i не является независимой от события $\{\nu \geqslant i\}$, даже когда все статистики ошибочных состояний одинаково распределены. Если, например, $i=N$, то тот факт, что $N-1$ состояний уже были отвергнуты, увеличивает вероятность того, что N-е состояние будет правильным. Так как число наблюдаемых, необходимых для решения, является функцией проверяемого состояния, то это будет влиять на значение $E(M_i|\nu \geqslant i)$. Однако если $\alpha \to 1$, то зависимость от проверяемого состояния не существует. Так как все состояния (правильное и неправильное) отвергаются с вероятностью, равной единице, то вероятность того, что i-е состояние является либо правильным состоянием источника, либо каким-либо заданным ошибочным состоянием, не изменяется предыдущими $i-1$ наблюдениями. В этом случае

$$E(M_i \mid \nu \geqslant i) = E(M_i) = \frac{1}{N} \sum_{j=0}^{N-1} E(M_i \mid j), \tag{2.41}$$

где j — индекс правильного состояния. Так как множество плотностей распределения $\{p(z^{(i)}|j),\ j=0, 1, \ldots, N-1\}$ не зависит от i, то эта независимость сохраняется для $E(M_i)$. Следовательно, из ф-лы (2.26) получаем

$$E(M_i) = E(M_0) \triangleq \frac{1}{N} \sum_{j=0}^{N-1} \frac{P_j \log A + (1-P_j) \log B}{E(z^{(0)} \mid j)}, \tag{2.42}$$

где P_j — вероятность принятия правильным нулевого состояния, когда источник находится в j-м состоянии. Из равенств (2.40) — (2.42) при $\alpha \to 1$ следует, что

$$E(M_T) = \frac{1}{N} \sum_{i=1}^{\infty} P(\nu \geqslant i) \sum_{j=0}^{N-1} E(M_0 \mid j) =$$

$$= \frac{E(\nu)}{N} \sum_{j=0}^{N-1} \frac{P_j \log A + (1-P_j) \log B}{E(z^{(0)} \mid j)}. \tag{2.43}$$

Но согласно гипотезе $P_0=(1-\alpha)$ и $P_j \leqslant \beta$ для всех $j \neq 0$. Более того, из соотношения (2.32) при $P_e \ll 1$ имеем: $E(\nu) \approx N\alpha/(1-\alpha)$, и эта величина фактически не зависит от вероятностей P_j, $j \neq 0$. Таким образом, если $A=(1-\alpha)/\beta$ и $B=\alpha/(1-\beta)$ и если $\alpha \to 1$, $\beta \to 0$ так, что верно соотношение (2.29) (при $P_e \ll 1$), то

$$E(M_T) = \sum_{j=1}^{N-1} \frac{1}{|E(z^{(0)} \mid j)|} + \frac{\left(\log \dfrac{N-1}{P_e} - 1\right)}{E(z^{(0)} \mid 0)}. \tag{2.44}$$

(Ср. этот результат с приведенным в табл. 2.1 для тех же самых условий.) Выражение для P_e, конечно, является верхней границей для действительной вероятности ошибки, так как соотношение (2.29) было выведено для случая, когда $P_j=\beta$ для всех $j\neq 0$.

В другом крайнем случае, когда α и β являются малыми $[\alpha=P_e/2,\ \beta=P_e/(N-1)]$, приближенное выражение для $E(M_T)$ можно получить, используя соотношение

$$E(M_i\,|\,\nu\geqslant i)\approx\sum_{j=i}^{N}E(M_i\,|\,j)\,P(j\,|\,\nu\geqslant i)\approx\sum_{j=i}^{N}\frac{1}{N+1-i}\,E(M_i\,|\,j),\tag{2.45}$$

где j снова обозначает индекс правильного состояния, а $P(j\,|\,\nu\geqslant i)$ — вероятность того, что j-е состояние является правильным при условии $\{\nu\geqslant i\}$. Это приближение справедливо потому, что с большой вероятностью состояние принимается тогда и только тогда, когда оно является правильным. По той же самой причине $P(\nu\geqslant i)\approx(N+1-i)/N$, $i=1,\ 2,\ \ldots,\ N$. Объединяя равенства (2.40) и (2.45) и используя эту последнюю аппроксимацию, находим, что

$$E(M_T)\approx\frac{1}{N}\sum_{i=1}^{N}\sum_{j=i}^{N}E(M_i\,|\,j).\tag{2.46}$$

Это выражение допускает дальнейшие упрощения, если плотность распределения $p(z^{(i)}\,|\,j)$ является функцией лишь разности $i-j$ по модулю N; при этом

$$E(M_T)\approx\frac{1}{N}\sum_{k=0}^{N-1}\sum_{i=1}^{N-k}E(M_0\,|\,k)=\sum_{k=0}^{N-1}\frac{N-k}{N}\,E(M_0\,|\,k).\tag{2.47}$$

Наконец, так как $P_0=1-\alpha$ и $P_j\leqslant\beta$ для всех $j\neq 0$ и так как α и β являются малыми $[\alpha=P_e/2,\ \beta=P_e/(N-1),\ P_e\ll 1]$, то

$$E(M_0\,|\,j)=\frac{P_j\log A+(1-P_j)\log B}{E(\,z^{(0)}\,|\,j)}\approx\begin{cases}\dfrac{\log\dfrac{2}{P_e}}{|E(\,z^{(0)}\,|\,j)|}, & j\neq 0;\\[2ex] \dfrac{\log\dfrac{N-1}{P_e}}{E(\,z^{(0)}\,|\,0)}, & j=0\end{cases}$$

и

$$E(M_T)\approx\log\frac{2}{P_e}\sum_{k=1}^{N-1}\frac{N-k}{N}\,\frac{1}{|E(\,z^{(0)}\,|\,k)|}+\frac{\log\dfrac{N-1}{P_e}}{E(\,z^{(0)}|\,0)}=$$

$$=\frac{1}{2}\log\frac{2}{P_e}\sum_{k=1}^{N-1}\frac{1}{|E(\,z^{(0)}\,|\,k)|}+\frac{\log\dfrac{N-1}{P_e}}{E(\,z^{(0)}\,|\,0)},\tag{2.48}$$

где последнее выражение справедливо при принятых здесь предположениях из-за того, что $E(z^{(0)}|k)=E(z^{(0)}|N-k)$. Снова P_e является верхней границей для действительной вероятности ошибки.

2.7. Об оптимальном последовательном поиске

Казалось бы, что для минимизации времени поиска вероятность ошибочного отвержения α должна быть взята малой для того, чтобы можно было выбрать правильное состояние с высокой вероятностью в момент проверки (или, в случае непрерывно продолжаемого поиска, для того, чтобы не отвергнуть его). В действительности табл. 2.1 показывает, что справедливо как раз противоположное. При дифференцировании математического ожидания времени поиска по α можно увидеть, что оно будет монотонно убывающей функцией α для всех значений N ($N \geqslant 2$) как в случае обычного, так и непрерывно продолжаемого последовательных поисков. Математическое ожидание величины M_T изображено на рис. 2.1 как функция α, когда $N\mu_0/\mu_1$ велико, а P_e мало по сравнению с единицей (см. табл. 2.1). Заметим, что в тех же самых условиях математические ожидания времени поиска для обычного и непрерывно продолжаемого поисков совпадают.

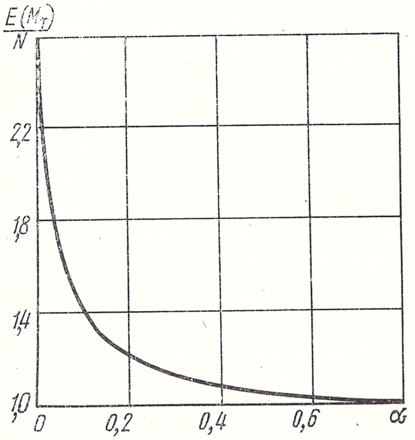


Рис. 2.1. Математическое ожидание времени последовательного поиска как функция α

Следует подчеркнуть, что когда $\alpha \to 1$, число проверок каждого состояния в процессе поиска стремится к бесконечности. Время поиска остается конечным, потому что одновременно стремится к нулю время исследования каждого состояния. Тем не менее это обстоятельство накладывает некоторые очевидные ограничения на процедуру поиска. Прежде всего, мы молчаливо предполагали, что по своей природе наблюдаемые являются непрерывными; каждое состояние могло проверяться вплоть до момента, когда его отношение плотностей вероятностей становилось меньше α и в этот момент наблюдение мгновенно прекращалось. На практике наблюдаемые часто являются дискретными (M — целое число) и, следовательно, по меньшей мере одна наблюдаемая должна быть в наличии, прежде чем может быть принято решение. Этот эффект квантования приводит к тому, что число наблюдений для каждого состояния не стремится к нулю при $\alpha \to 1$. Далее предполагалось, что при переходе от исследования одного состояния к другому время не затрачивается. Предположим, что t_0 секунд затрачиваются, чтобы выполнить каждое наблюдение, и t_1 секунд в действительности необходимы, чтобы перейти от одного состояния к другому. При этом математическое ожидание времени поиска

$$E(T_s) = E(\nu - 1)\, t_1 + E(M_T)\, t_0. \tag{2.49}$$

Когда $\alpha \to 1$, первое слагаемое обращается в бесконечность независимо от того, насколько малым является t_1, если оно отлично от нуля. Тем не менее результаты, относящиеся к случаю, когда $\alpha \to 1$, остаются полезными при отыскании ожидаемых границ для параметров, относящихся к работе идеальной схемы. Более того, тест все еще остается полезным даже, если α несколько меньше единицы и, как следствие, время, затрачиваемое на проверку каждого состояния, не стремится к нулю, а число проверок не стремится к бесконечности [ср. равенство (2.31)]. Оба упомянутые выше возражения снимаются, по крайней мере до некоторой степени, когда α несколько меньше единицы. Если время t_1, необходимое для перехода от исследования одного состояния к другому, известно, то фактически возможно определить оптимальное значение α. Часто, однако, значение t_1 является настолько малым, что оптимальное значение α, удовлетворяющее этому уравнению, слишком близко к единице, что не позволяет оправдать пренебрежение эффектом квантования. В любом случае увеличение времени, вызываемое отклонением α от единицы, не является чрезмерным, как можно увидеть из рис. 2.1.

Среднее число наблюдаемых, необходимых для каждого теста, можно определить с помощью результатов § 2.3. Когда это число достигает, скажем, десяти, то с достаточным основанием можно считать, что эффект квантования не играет больше роли.

С этими оговорками математическое ожидание времени, необходимого для завершения последовательного поиска, минимизируется при вероятности ошибочного отклонения, стремящейся к единице. В этом смысле последовательный поиск с $\alpha = 1$ является оптимальным среди рассматриваемого класса процедур поиска. Но можно ли сказать, что этот метод будет оптимальным в каком-либо более широком смысле? Или какой алгоритм поиска в более общем случае минимизирует математическое ожидание времени поиска, если только одно состояние может быть проверено за один раз?

Хотя наиболее общий ответ на этот вопрос представляется неясным, следующее правило является заманчивым, правда, не всегда удачным конкурентом оптимальной стратегии (см. задачу 2.7): всегда проверять состояние, имеющее наибольшую *текущую* вероятность быть правильным. Предположим, что вероятности μ-го состояния θ_μ и ν-го состояния θ_ν в один и тот же момент поиска равны P_μ и P_ν соответственно и $P_\mu = P_\nu \geqslant P_i$ для всех $i \neq \mu, \nu$. При этом мы производим наблюдение $y_j^{(\nu)}$, относящееся к ν-му состоянию. Тогда, если

$$p(y_j^{(\nu)} \mid \theta_l) = \begin{cases} p_0(y_j^{(\nu)}), & l = \nu; \\ p_1(y_j^{(\nu)}), & l \neq \nu. \end{cases}$$

то новая вероятность ν-го состояния

$$P'_\nu = \frac{p_0\left(y_j^{(\nu)}\right) P_\nu}{p_0\left(y_j^{(\nu)}\right) P_\nu + p_1\left(y_j^{(\nu)}\right)(1-P_\nu)} = \frac{P_\nu}{P_\nu + \frac{1}{\lambda_{\nu j}}(1-P_\nu)}, \qquad (2.50)$$

где $\lambda_{\nu j} = p_0(y_j^{(\nu)})/p_1(y_j^{(\nu)})$ — отношение правдоподобия. Если P'_ν меньше, чем P_μ, то μ-е состояние становится наиболее вероятным. Таким образом, если правило обязательной проверки текущего наиболее вероятного состояния применено, то исследование ν-го состояния на этот раз будет прекращено. Но P'_ν меньше, чем P_ν, тогда и только тогда, когда $\lambda_{\nu j}$ меньше единицы. Если $\lambda_{\nu j}$ больше единицы, то ν-е состояние остается наиболее вероятным состоянием, и его исследование продолжается. Фактически оно продолжается до тех пор, пока произведение $\lambda_{\nu j}\lambda_{\nu, j+1}\lambda_{\nu, j+2} \dots \lambda_{\nu, j+l}$ не станет меньше единицы. Условие, что в процедуре поиска всегда исследуется наиболее вероятное состояние, реализуется, следовательно, в последовательном поиске с нижним порогом $B=\alpha/(1-\beta)$, равным единице. Соответственно последовательный поиск с $\alpha=1-\beta$ [и, следовательно, согласно (2.29) с $\alpha\approx 1$] можно рассматривать как алгоритм, реализующий эту интуитивно привлеченную стратегию.

2.8. Проверка многих гипотез

Если те или другие ограничения, например, связанные со сложностью вычислений, не являются решающими, то часто выгодно выполнить проверку многих гипотез, одновременно проверяя все конкурирующие гипотезы, вместо того, чтобы осуществлять поиск, который, вообще говоря, требует затраты большего времени. В этом параграфе кратко рассмотрены некоторые аспекты проверки многих гипотез как для процедуры с фиксированным объемом выборки, так и для процедуры последовательного типа. Снова рассмотрение ограничено только простыми гипотезами. Обобщение на сложные гипотезы во многих случаях является непосредственным.

Тесты с фиксированными объемами выборок. Если тест следует закончить в заранее установленное время (т. е. если должно быть произведено фиксированное число наблюдений), то оптимальный тест легко получить, обобщая результаты § 2.2. Пусть опять C_{ij} обозначает стоимость принятия гипотезы H_i $(\theta=\theta_i)$, когда правильной гипотезой является H_j $(\theta=\theta_j)$. Тогда математическое ожидание стоимости решения будет

$$E(\text{стоимость}) = \sum_j \sum_i C_{ij} P(H_j) \int_{R_i} p(Y \mid H_j)\, dY, \qquad (2.51)$$

где R_i — область принятия гипотезы H_i. Используя правило Байеса и меняя порядок интегрирования и суммирования, получаем

$$E(\text{стоимость}) = \sum_i \int_{R_i} \sum_j C_{ij} P(H_j \mid Y)\, p(Y)\, dY. \qquad (2.52)$$

Математическое ожидание стоимости минимизируется поэтому при включении Y в область R_ν тогда и только тогда, когда выражение

$$\sum_j C_{ij} P(H_j \mid Y) \tag{2.53}$$

достигает своего минимального значения при $i=\nu$. Таким образом, ν-я гипотеза H_ν принимается тогда и только тогда, когда

$$\frac{\sum\limits_j C_{\nu j} P(H_j \mid Y)}{\sum\limits_j C_{ij} P(H_j \mid Y)} = \frac{\sum\limits_j C_{\nu j}\, p(Y \mid H_j)\, P(H_j)}{\sum\limits_j C_{ij}\, p(Y \mid H_j)\, P(H_j)} < 1 \tag{2.54}$$

для всех $i \neq \nu$. Эта процедура представляет собой *байесовский тест* для случая многих гипотез [ср. с равенством (2.4)].

Опять возникают трудности при определении оптимального теста в случае, когда неизвестны либо стоимости, либо априорные вероятности $p(H_i)$, либо и то, и другое. Ограничимся рассмотрением случая, когда известны все априорные вероятности и стоимости всех ошибочных решений равны между собой:

$$C_{ij} = \begin{cases} C_0, & i = j; \\ C_1, & i \neq j. \end{cases}$$

Требуется минимизировать выражение

$$\sum_j C_{ij} P(H_j \mid Y) = C_1 \sum_j P(H_j \mid Y) - (C_1 - C_0) P(H_i \mid Y) =$$
$$= C_1 \sum_j P(H_j \mid Y) - (C_1 - C_0) \frac{p(Y \mid H_i)\, P(H_i)}{P(Y)}. \tag{2.55}$$

Стоимость минимизируется (если $C_1 > C_0$) выбором той гипотезы H_i, для которой вероятность

$$p(Y \mid H_i)\, P(H_i) \tag{2.56}$$

принимает максимальное значение. Эта процедура, очевидно, является *тестом максимальной апостериорной вероятности* для многих гипотез.

Обозначая через ξ_ν случайную величину $p(Y \mid H_\nu) P(H_\nu)$, можно выразить вероятность ошибки в принятии решения этого типа следующим образом:

$$P_e = \sum_{\mu=1}^{N} P(H_\mu)\, P_e(\mu), \tag{2.57}$$

где $P_e(\mu) = 1 - \Pr\left\{ \xi_\mu > \max\limits_{\nu \neq \mu} \xi_\nu \mid H_\mu \right\} =$

$$= 1 - \int_0^\infty \int_0^{\xi_\mu} \ldots \int_0^{\xi_\mu} p(\xi_1, \xi_2, \ldots, \xi_N \mid H_\mu)\, d\xi_1\, d\xi_2 \ldots d\xi_N\, d\xi_\mu.$$

Подынтегральным выражением является условная совместная плотность распределения вероятности случайных величин ξ_ν. Так как эти величины обычно не являются независимыми, то точное вычисление вероятности ошибки часто затруднительно. Тем не менее можно оценить эту вероятность. Одну из таких границ можно получить, если учесть, что

$$\max_{i\neq\mu} \Pr\{\xi_i - \xi_\mu \geqslant 0 \mid H_\mu\} \leqslant P_e(\mu) \leqslant \sum_{\substack{i=1\\ i\neq\mu}}^{N} \Pr\{\xi_i - \xi_\mu \geqslant 0 \mid H_\mu\}.$$

Так как $\Pr\{\xi_i - \xi_\mu \geqslant 0 \mid H_\mu\} = \Pr\{\xi_\mu/\xi_i \leqslant 1 \mid H_\mu\}$ (члены ξ_i являются плотностями распределений и, следовательно, не могут быть отрицательными), то

$$\max_{i\neq\mu} \int\limits_{\lambda_{\mu i}\leqslant r_{\mu i}} p(Y \mid H_\mu)\, dY \leqslant P_e(\mu) \leqslant$$

$$\leqslant \sum_{\substack{i=1\\ i\neq\mu}}^{N} \int\limits_{\lambda_{\mu i}\leqslant r_{\mu i}} p(Y \mid H_\mu)\, dY \leqslant N \max_{i\neq\mu} \int\limits_{\lambda_{\mu i}\leqslant r_{\mu i}} p(Y \mid H_\mu)\, dY, \qquad (2.58)$$

где $\lambda_{\mu i} = \dfrac{p(Y \mid H_\mu)}{p(Y \mid H_i)}$ и $r_{\mu i} = \dfrac{P(H_i)}{P(H_\mu)}$.

Последовательные тесты. Чтобы иметь возможность проводить последовательный тест для многих гипотез, нужно както определить отношение плотностей вероятностей вида

$$\frac{p(Y(m) \mid H_j)}{(Y(m) \mid H_j^*)} \qquad (2.59)$$

для каждой гипотезы H_j. Альтернативная гипотеза H^*_j может быть одной из конкурирующих гипотез, но может и не совпадать ни с одной из них. Например, плотность распределения вероятности $p(Y|H^*_j)$ может представлять собой некоторое взвешенное среднее плотностей распределений, соответствующих всем альтернативным гипотезам, т. е.

$$p(Y(m) \mid H_j^*) = \sum_{i\neq j} w_i(m)\, p(Y(m) \mid H_i), \qquad (2.60)$$

где $\sum\limits_{i\neq j} w_j(m) = 1$. Мы указывали на зависимость весов w_i от числа наблюдаемых в множестве $Y(m)$. Тест, который проводится параллельно, включает в себя одновременную проверку всех гипотез H_j до тех пор, пока все гипотезы, кроме одной, не будут отвергнуты; следовательно, одной из форм, которую эта зависимость может принять, является равенство $w_i(m)=0$, если H_i уже была отвергнута. В только что упомянутом последовательном тесте для многих гипотез все отношения (2.59) рассматриваются одновременно, и гипотеза H_j отвергается, как только соответствующее отношение становится меньше некоторого порога B_j. Отсюда следует, что

$$\alpha_\mu = \sum_{m=1}^{\infty} \int\limits_{\overline{R}_\mu(m)} p(Y(m) \mid H_\mu)\, dY(m) =$$

$$= B_\mu \sum_{m=1}^{\infty} \int\limits_{\overline{R}_\mu(m)} p(Y(m) \mid H_\mu^*)\, dY(m),$$

где $\overline{R}_\mu(m)$ — область отвержения μ-й гипотезы, определяемая отношениями (2.59). Независимо от альтернативной гипотезы H_μ^* события, по которым производится суммирование в первой части этого равенства, являются взаимоисключающими; если $Y(m)$ принадлежит $\overline{R}_\mu(m)$, то $Y(l)$ не принадлежит $\overline{R}_\mu(l)$ для любых $l<m$ или проверка μ-го состояния завершена до того, как произведено m-е наблюдение. Следовательно, эта сумма не превышает единицу,

$$\alpha_\mu \leqslant B_\mu, \tag{2.61}$$

и вероятность ошибочного отвержения гипотезы H_μ ограничена значением порога B_μ. К сожалению, в общем случае трудно определить математическое ожидание числа наблюдаемых, необходимых для завершения последовательного теста многих гипотез. Большинство относящихся сюда результатов получены эмпирически.

2.9. Оценка статистических параметров

Существенное отличие оценивания статистических параметров от проверки статистических гипотез состоит в том, что, по предположению, гипотезы образуют лишь дискретное множество, в то время как параметры могут в общем случае принимать континуум значений. Рассмотрим задачу оценивания одного единственного параметра x по наблюдаемым Y. Чтобы обобщить методы вычисления математического ожидания стоимости решения в случае многих гипотез и сделать их пригодными при оценивании параметра, необходимо только определить *стоимостную функцию* $C(\hat{x}, x)$, которая указывает стоимость принятия оценки $\hat{x} = \hat{x}(Y)$, когда параметр в действительности равен x. Далее, видоизменяя равенство (2.52) применительно к рассматриваемой ситуации, получаем

$$E\,(\text{стоимость}) = \int E\,(\text{стомость} \mid Y)\, p\,(Y)\, d\,Y, \tag{2.62}$$

где $E\,(\text{стоимость} \mid Y) = \int C(\hat{x},\ x)\, p(x \mid Y) dx$. Таким образом, для каждого Y, для которого $p(Y) \neq 0$, нужно определить оценку $\hat{x}(Y)$, так, чтобы E(стоимость $|\, Y$) было минимальным. Такие оценки называются *байесовскими оценками.*

Одной из наиболее широко используемых стоимостных функций является квадрат ошибки оценки:

$$C(\hat{x} - x) = (\hat{x} - x)^2. \tag{2.63}$$

Легко видеть, что для этой стоимостной функции оптимальной оценкой $\hat{x}$ величины x является ее условное математическое ожидание

$$\hat{x} = E(x \,|\, Y). \tag{2.64}$$

Рассмотрим любую другую оценку $\tilde{x}$, тогда

$$E\,(\text{стоимость} \,|\, Y) = E\left((\tilde{x} - x)^2 \,|\, Y\right) =$$

$$= E\left[\left((\tilde{x} - \hat{x}) - (x - \hat{x})\right)^2 | \, Y\right] = (\tilde{x} - \hat{x})^2 +$$

$$+ E\left[(x - \hat{x})^2 \,|\, Y\right] \geqslant E\left[(x - \hat{x})^2 \,|\, Y\right],$$

где равенство выполняется только при $\tilde{x} = \hat{x}$. Можно показать, что при некоторых довольно общих ограничениях на плотность распределения $p(x\,|\,Y)$ условное математическое ожидание $E(x\,|\,Y)$ является оптимальной формулой оценки[1]) для весьма широкого класса стоимостных функций. В частности, это утверждение справедливо, если стоимостная функция является симметричной функцией разности $\hat{x}$—x, неубывающей функцией ее абсолютного значения и если плотность $p(x\,|\,Y)$ является унимодальной и симметричной относительно своего среднего значения. Но если плотность $p(x\,|\,Y)$ унимодальна и симметрична относительно среднего значения, то ясно, что

$$\max_x p(x \,|\, Y) = p(\hat{x} \,|\, Y), \tag{2.65}$$

где $\hat{x} = E(x\,|\,Y)$, т. е. условное среднее значение x равно условной моде распределения x. Соответственно оптимальная формула оценки в этих условиях является *формулой оценки по максимуму апостериорной вероятности.*

При оценивании статистических параметров так же, как при проверке гипотез, могут быть неизвестны априорные вероятности, и, как и там, выбор критерия для формулы оценки в отсутствии этой информации является менее очевидным. Часто используются следующие меры при вычислении формул оценок:

---

[1]) Термин *«формула оценки»* используется для обозначения функции $\hat{x} = \hat{x}(Y)$. Оценка величины x есть значение $\hat{x}$ для любого заданного множества Y. *(Прим. авт.)*

1. *Смещение* оценки. Если $\hat{x}$ является оценкой x и $E(\hat{x}|x)=$ $=x+b(x)$, то $b(x)$ называется смещением оценки $\hat{x}$.

2. Условная дисперсия $E[(\hat{x}-x-b(x))^2|x]$ оценки. Любая оценка $\hat{x}$ величины x, основанная на множестве независимых одинаково распределенных наблюдаемых $Y=\{y_i\}$ $(i=1,\ 2,\ \ldots,\ N)$, имеет дисперсию, для которой граница снизу определяется выражением

$$E\,[(\hat{x}-x-b\,(x))^2\,|\,x]\geqslant\frac{\left(1+\dfrac{d\,b\,(x)}{dx}\right)^2}{NE\left[\left(\dfrac{\partial\log p\,(y\,|\,x)}{\partial x}\right)^2\middle|\,x\right]}\,, \tag{2.66}$$

где $p(y|x)=p(y_i|x)$ — условная плотность распределения наблюдаемых y_i. Это неравенство называется неравенством Крамера—Рао.

В большинстве случаев предпочтительна оценка, которая является несмещенной и которая среди всех несмещенных оценок имеет дисперсию, достигающую нижней границы (2.66). Такие оценки называются *эффективными.* В связи с этим *оценка максимального правдоподобия*, т. е. корень (или корни) ¹) *x уравнения правдоподобия*

$$\frac{\partial}{\partial x}\log p\,(Y\,|\,x)=0, \tag{2.67}$$

имеет два весьма привлекательных свойства. Первое — если существует эффективная оценка, то она является оценкой максимального правдоподобия. Второе — даже если эффективная оценка не существует, то существует оценка максимального правдоподобия, которая является *асимптотически эффективной*, когда число наблюдаемых становится большим.

Принцип максимума правдоподобия, использованный в предыдущих параграфах этой главы, в рассматриваемой ситуации состоял бы в выборе в качестве оценки x такой величины, которая максимизирует в области допустимых значений x функцию $p(Y|x)$ [или, что эквивалентно, функцию $\log p(Y|x)$]. Эта оценка часто является решением уравнения правдоподобия, но, конечно, не всегда (например, уравнение правдоподобия может не иметь решения в рассматриваемой области значений x). Кроме того, уравнение правдоподобия может иметь решения, которые не максимизируют $p(Y|x)$. Для того чтобы в дальнейшем изложении

---

¹) Иногда случается так, что $p(Y|x)$ принимает максимальное значение при некотором x, не зависящем от Y. Такие оценки обычно отбрасываются в пользу некоторой другой оценки $\hat{x}=\hat{x}(Y)$, которая является функцией Y и для которой $p(Y|x)$ достигает, по меньшей мере, относительного максимума. *(Прим. авт.)*

различать между собой эти две формулы оценок, мы будем называть любую формулу оценки, основанную на максимуме функции $p(Y|x)$, формулой оценки *по принципу максимума правдоподобия* и резервировать термин «формула оценки максимального правдоподобия» для тех формул оценок, которые определяются равенством (2.67).

Распространение результатов на более общий случай, когда несколько параметров должны быть оценены одновременно, во многом является очевидным. Неизвестный параметр x теперь становится вектором $\mathbf{x}=(x_1, x_2, \ldots, x_m)$. Оценки параметров $x_1, x_2, \ldots, x_m$ по максимуму апостериорной вероятности, например, при заданных наблюдаемых $Y=\{y_i\}$ — это величины, которые одновременно максимизируют выражение

$$p(\mathbf{x}\,|\,Y)=p(x_1, x_2,\ldots, x_m\,|\,Y), \tag{2.68}$$

в то время как оценки максимального правдоподобия — это величины x_i, которые удовлетворяют уравнениям [1]:

$$\frac{\partial}{\partial x_i}p(Y\,|\,x_1, x_2,\ldots, x_m)=0, \quad i=1, 2,\ldots, m. \tag{2.69}$$

Задачи

2.1. Пусть S — двоичный источник; его выход представляет собой последовательность статистически независимых *нулей* и *единиц* с $\Pr(0)=1-\Pr(1)=p$. Следует определить, используя шесть последовательных выходных символов источника S, находится ли он в состоянии θ_0 с $p=2/3$ или в состоянии θ_1 с $p=1/2$. Показать, что в каждой из следующих ситуаций соответствующим образом выбранный тест принимает гипотезу H_0, что $\theta=\theta_0$ тогда и только тогда, когда число появившихся *нулей* больше некоторого числа ν, и определить ν в каждом случае. (Обозначения здесь такие же, как в § 2.2):

а) $P(H_0)=P(H_1)=1/2$; $C_{01}-C_{11}=C_{10}-C_{00}$;
б) $P(H_0)=P(H_1)=1/2$; $C_{01}-C_{11}=1$; $C_{10}-C_{00}=10$;
в) $P(H_0)=P(H_1)=1/2$; $C_{01}-C_{11}=10$; $C_{10}-C_{00}=1$;
г) α не превосходит 1/9;
д) $C_{11}=C_{00}=0$, $C_{01}=1$, $C_{10}=10$; априорные вероятности неизвестны.

Определить α и β в каждом случае.

2.2. а) Указать последовательный тест отношения плотностей вероятностей для определения состояния источника, описанного в предыдущей задаче. Найти среднее и дисперсию числа выходных символов источника, необходимых для последовательного решения с $\alpha=\beta=1/3$. (Обратить внимание, что в этих условиях влияние «перескоков границ» существенно, так что ответы будет лишь приближенными.)

---

[1] При одновременной оценке нескольких параметров минимальная возможная дисперсия оценки некоторого частного параметра Φ_i может быть больше, чем в случае, когда имеется единственный неизвестный параметр. В частности, если методом максимума правдоподобия оцениваются два параметра Φ_1 и Φ_2, то асимптотические дисперсии этих двух оценок будут больше, чем значения, задаваемые ф-лой (2.66), до тех пор, пока оба этих параметра не станут независимыми в том смысле, что

$$E\left(\frac{\partial \log p(y\,|\,\Phi_1,\ \Phi_2)}{\partial \Phi_1}\ \frac{\partial \log p(y\,|\,\Phi_1,\ \Phi_2)}{\partial \Phi_2}\right)=0.$$

(Прим. авт.)

б) Предположим, что источник на самом деле выдает *нули* с вероятностью 5/12. Найти вероятность принятия при этих условиях гипотезы H_0 и определить математическое ожидание числа наблюдений, необходимых для завершения теста.

2.3. Какие условия накладывает минимаксный критерий на пороговые значения в последовательном тесте?

2.4. Используя тождество Вальда, показать, что если $E(z|\theta)=0$, $\operatorname{var}(z|\theta)\neq 0$, то равенства (2.25) и (2.26) переходят соответственно в

$$P(0)=\frac{\log B}{\log B-\log A} \text{ и } E(M\,|\,\theta)=\left|\frac{\log A\log B}{\operatorname{var}(z\,|\,\theta)}\right|.$$

2.5. При последовательном поиске нужно определить состояние θ источника. Распределение наблюдаемых z известно и задается плотностью $p_0(z)$, если состояние источника является тем, которое в действительности проверяется, и плотностью $p_1(z)$ во всех остальных случаях. Эта ситуация отличается от рассмотренной в § 2.6, где априорная вероятность того, что источник находится в состоянии θ_i, равна P_0 для всех i (P_0 — произвольная вероятность, не превосходящая $1/N$). Поиск вводится для того, чтобы с вероятностью ошибки P_e определить правильное состояние источника, когда оно в действительности является одним из проверяемых. Показать, что когда $\alpha\to 1$, $\beta\to 0$ при условии, определяемом равенством (2.27), математическое ожидание числа наблюдений, необходимых, чтобы завершить поиск (ср. с табл. 2.1),

$$E(M_T\,;\ P_0)=E\left(M_T\,;\ \frac{1}{N}\right)+(1-P_e)(1-NP_0)\times$$
$$\times\left\{\frac{A^*-1-\log A^*}{\mu_1}-\frac{\log A^*-\dfrac{A^*-1}{A^*}}{\mu_0}\right\}.$$

Показать, что выражение, стоящее в правой части равенства, является положительным при условии, что можно пренебречь «эффектом квантования», упомянутым на стр. 40.

2.6. а) Поиск, описанный в предыдущей задаче, следует модифицировать, завершая его либо когда $P_i(M)\geqslant P_c$ для некоторого i, либо когда $P_i(M)\leqslant P_r$ для всех i ($i=1,\ 2,\ \ldots,\ N$), где $P_i(M)$ — апостериорная вероятность того, что после M наблюдений источник находится в состоянии i. Показать, что если поиск построен так, чтобы проверять наиболее вероятное состояние в каждый момент, то математическое ожидание требуемого числа наблюдений

$$E(M_T\,;\ P_0,\ P_r,\ P_c)=\int\limits_{P_r}^{P_0}E(M_T\,;\ x)\,p(x)\,dx,$$

где $E(M_T;\ x)$ определено в задаче 2.5, но с
$A^*\to A^*(x)=(1-x)P_c/x(1-P_c)$, $P_e=1-P_c$ и где $p(x)=dP(x)/dx$ с

$$P(x)=\exp\left\{-\int\limits_{x}^{P_0}\frac{(1-\xi)}{P_c-\xi}\,\frac{N}{1-N\xi}\,d\xi\right\}.$$

Указание. Рассмотреть ряд усеченных последовательных поисков; i-й поиск проводится с верхним и нижним порогами A_i и B_i соответственно, и усечение производится не только тогда, когда одна из статистик теста достигает A_i, но также тогда, когда все N статистик теста достигают B_i. Показать, что математическое ожидание числа наблюдений, необходимых для завершения такого поиска, равно произведению $1-\Pr(B_i|A_i,\ B_i)$ на математическое ожидание числа наблюдений, необходимых для завершения соответствующего неусеченного поиска, где $\Pr(B_i|A_i,\ B_i)$ — вероятность того, что все N статистик теста достигнут нижнего порога. Далее показать, что если P_i обозначает апостериорную вероятность каждого из проверяемых состояний в конце i-го усеченного поиска, если $A_i \triangleq$ $\triangleq (1-P_{i-1})P_c/P_{i-1}(1-P_c)$, $B_i \triangleq (1-P_{i-1})(P_{i-1}-\Delta_{i-1})/P_{i-1}(1-P_{i-1}+\Delta_{i-1})$ и если $\Delta_i=(1-P_i)\Delta/(1-NP_i)$, то при $\Delta\to 0$ имеем: $P_i\to P_0-i\Delta$. Сформулированный результат теперь получается, если взять предел при $\Delta\to 0$ взвешенной суммы математического ожидания числа наблюдений, необходимых, чтобы завершить каждый последовательный усеченный поиск; веса определяются вероятностью того, что поиск должен закончиться решением.

б) Используя результат п. а), вывести выражение для математического ожидания числа наблюдений, необходимых для завершения последовательного поиска, когда априорные вероятности различных состояний не равны.

2.7. Один из методов определения, находится ли источник в состоянии θ_0 или в состоянии θ_1, когда априорная вероятность того, что каждое состояние является правильным, равна 1/2, состоит просто в проверке одного из состояний до тех пор, пока его апостериорная вероятность достигнет либо P_c, либо $1-P_c$. Сравнить эту стратегию (используя математическое ожидание числа наблюдений, необходимых для завершения теста) со стратегией последовательного поиска, описанной в § 2.7. При каких условиях последняя будет лучше? Является ли более эффективной стратегия, которая всегда проверяет *менее* вероятное из двух состояний?

2.8. Пусть $Y=\{y_i\}$ — множество N независимых выборок случайной величины y с

$$p(y)=\left(1/\sqrt{2\pi}\sigma\right)\exp\{-(y-\mu)^2/2\sigma^2\},$$

но с неизвестными μ и σ. Найти оценки наибольшего правдоподобия для μ, σ и σ^2. Являются ли эти оценки смещенными? Эффективны ли они?

Глава 3

НЕПРЕРЫВНЫЕ ПО АМПЛИТУДЕ И ДИСКРЕТНЫЕ ПО ВРЕМЕНИ СИСТЕМЫ СВЯЗИ

3.1. Введение

В этой и следующей главах рассмотрены некоторые системы связи, наиболее интересные с точки зрения синхронизации; все эти системы будем называть *импульсными* или *дискретными по времени системами связи.* В таких системах в течение интервала времени $iT_s<t<(i+1)T_s$ передается сигнал, описываемый одной из функций, принадлежащих некоторому множеству; эта конкретная функция определяется источником информации.

Импульсные системы связи могут быть разделены на два типа в зависимости от того, используется ли конечное (или бесконечное счетное) множество функций или несчетное бесконечное множество (например, множество функций может быть семейством функций времени, зависящих от некоторого непрерывного параметра). Второй тип импульсных систем связи — *непрерывные по амплитуде* системы — и является предметом этой главы. Рассмотрение систем первого типа, обычно называемых дискретными системами связи, проводится в гл. 4.

Системы связи, рассматриваемые в этой главе, включают в себя системы с когерентной амплитудной модуляцией, некогерентной импульсной амплитудной модуляцией и когерентной фазовой манипуляцией. Предполагается, что во всех этих системах принимаемый сигнал имеет вид:

$$y(t) = Ax(t-iT_s, \nu_i) + n(t), \quad iT_s < t < (i+1)T_s, \tag{3.1}$$

где ν_i — параметр, определяемый передаваемой информацией, а $n(t)$ — белый гауссовский шум с односторонней спектральной плотностью N_0. Источник предполагается стационарным, так что статистики сигнала $x(t-iT_s, \nu_i)$ не зависят от i. Целью рассмотрения является определение вида оптимального демодулятора и изучение общих характеристик этих систем. Для этого нужно, очевидно, выбрать некоторый критерий оптимальности и некоторые параметры, на основе которых будем сравнивать различные системы. Этим вопросам посвящен § 3.3. Еще более важной для обсуждения импульсных систем модуляции является заранее предполагаемая способность удовлетворительного представления информации последовательностью чисел, появляющихся со средней скоростью одно число за каждые T_s секунд. Если информация уже имеет эту дискретную по времени форму, то никаких фундаментальных проблем не возникает. Но если она является существенно непрерывной функцией времени, то ее необходимо как-то превратить в такую последовательность в надежде, что при этом потери информации будут минимальны. Один из методов такого преобразования обсуждается в следующем параграфе.

3.2. Теорема отсчетов

Пусть $f(t)$ представляет собой выборочную функцию стационарного случайного процесса. Обозначим через $b_\tau(t-\eta)$ периодическую функцию, изображенную на рис. 3.1. Импульсы шириной в τ секунд каждый расположены так, что их центрами являются моменты $t=\eta+iT$, $i=\ldots, -1, 0, 1, 2, \ldots$, где η — случайная величина с плотностью распределения

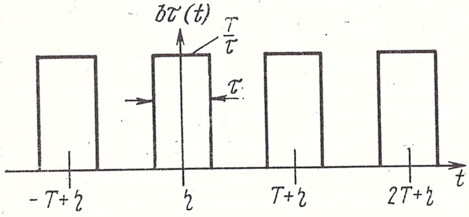


Рис. 3.1. Периодическая отсчетная функция

$$p(\eta)=\begin{cases}\dfrac{1}{T} & \text{при } 0\leqslant\eta\leqslant T;\\ 0 & \text{в остальных случаях.}\end{cases} \tag{3.2}$$

Так как функция $b_\tau(t-\eta)$ является периодической, то она может быть разложена в ряд Фурье:

$$b_\tau(t-\eta)=a_0+2\sum_{n=1}^{\infty}a_n\cos\omega_n(t-\eta), \tag{3.3}$$

где $a_0=1$; $a_n=(\sin\omega_n\tau)/\omega_n\tau$ и $\omega_n=2\pi n/T$.

Рассмотрим теперь произведение $g(t)=f(t)b_\tau(t-\eta)$. Если процесс $f(t)$ не зависит от η, то автокорреляционная функция произведения равна произведению автокорреляционных функций:

$$R_g(\gamma)=E\{f(t)f(t+\gamma)b_\tau(t-\eta)b_\tau(t-\eta+\gamma)\}=R_f(\gamma)R_b(\gamma). \tag{3.4}$$

Но

$$R_b(\gamma)=a_0^2+2\sum_{n=1}^{\infty}a_n^2\cos\omega_n\gamma. \tag{3.5}$$

Следовательно, спектральная плотность произведения имеет вид

$$S_g(\omega)=\int_{-\infty}^{\infty}R_g(\gamma)e^{-i\omega\gamma}d\gamma=\sum_{n=-\infty}^{\infty}a_n^2S_f(\omega-\omega_n), \tag{3.6}$$

где, по определению $a_{-n}=a_n$. Если спектральная плотность мощности $S_f(\omega)$ процесса $f(t)$ имеет вид, изображенный на рис. 3.2*а*, то $g(t)$ имеет спектральную плотность, показанную на рис. 3.2*б*.

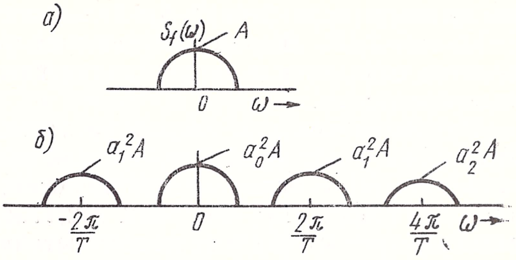


Рис. 3.2. Спектральные плотности мощности до и после отсчетов:
а) спектр сигнала; *б)* спектр отсчетов сигнала

Из этого рассуждения следует важное заключение, что если спектральная плотность $S_f(\omega)$ равна нулю для всех частот $|\omega/2\pi|\geqslant W$, как показано на рис. 3.2, то слагаемые в первой части равенства (3.6) не перекрываются по частоте при условии $W\leqslant 1/2T$. Отсюда следует, в принципе, возможность пропустить процесс $g(t)$ через фильтр, имеющий частотную характеристику

$$H(\mathrm{i}\,\omega)=\begin{cases}1, & |\omega|<2\pi W;\\ 0, & |\omega|>2\pi W,\end{cases}$$

и оставить только низкочастотное слагаемое $a^2{}_0S_f(\omega)=S_f(\omega)$. Но как раз этот член является спектральной плотностью процесса $f(t)$. Очевидно, что никакой потери информации в результате умножения $f(t)$ на функцию $b_\tau(t—\eta)$ не произошло, хотя функция $b_\tau(t—\eta)$ тождественно совпадает с нулем большую часть времени.

Так как два совершенно различных процесса могут иметь один и тот же спектр, то это утверждение требует дальнейшего обоснования. Чтобы дать это обоснование, нужно лишь рассмотреть среднеквадратическую разность между $f(t)$ и выходным сигналом фильтра.

Пусть $h(t)$ — импульсный отклик фильтра с характеристикой $H(\mathrm{i}\omega)$. Тогда

$$E\left\{f(t)-\int\limits_{-\infty}^{\infty}g(\gamma)\,h(t-\gamma)\,d\gamma\right\}^2=$$

$$=R_f(0)-2\int\limits_{-\infty}^{\infty}R_{fg}(\gamma-t)\,h(t-\gamma)\,d\gamma+$$

$$+\int\limits_{-\infty}^{\infty}\int\limits_{-\infty}^{\infty}R_g(\gamma_2-\gamma_1)\,h(t-\gamma_1)\,h(t-\gamma_2)\,d\gamma_1\,d\gamma_2=$$

$$=\int\limits_{-\infty}^{\infty}S_f(\omega)\,[1-2\,H(\mathrm{i}\,\omega)]\,\frac{d\omega}{2\pi}+\int\limits_{-\infty}^{\infty}S_g(\omega)\,|H(\mathrm{i}\,\omega)|^2\,\frac{d\omega}{2\pi}. \qquad (3.7)$$

(Заметим, что $R_{fg}(\alpha)=R_f(\alpha)\,E(b_\tau(t—\eta))=R_f(\alpha)$.) Это выражение тождественно равно нулю, если $H(\mathrm{i}\omega)$ определена так, как указано выше, и если $S_f(\omega) = S_g(\omega)$ для $|\omega| < \omega_m$ и $S_f(\omega) = 0$ для $|\omega| > \omega_m = 2\pi W$. В рассматриваемых условиях восстанавливаемый процесс совпадает в среднеквадратическом смысле с первоначальным процессом.

Заметим, что этот вывод не зависит от ширины импульса τ. Устремляя $\tau \to 0$, замечаем, что вся информация, содержащаяся в процессе $f(t)$ с ограниченной полосой, содержится в выборочных значениях $f(\eta + nT)$; $n = 0, \pm 1, \pm 2, \ldots$; $T = 1/2W$ для любого η. Отсюда следует, что сигнал может быть восстановлен с помощью пропускания последовательности выборок $g(t) = T \sum\limits_{n=-\infty}^{\infty} f(t)\delta(t - nT)$ [$\delta(t)$ — дельта-функция Дирака] через фильтр с импульсным откликом

$$h(t) = \frac{1}{2\pi} \int\limits_{-\infty}^{\infty} H(\mathrm{i}\,\omega)\, e^{\mathrm{i}\omega t}\, d\omega = (\sin 2\pi Wt)/\pi t.$$

Таким образом, если $f(t)$ имеет спектр мощности шириной W или меньше, то

$$(t) = \int\limits_{-\infty}^{\infty} g(\alpha)\, h(t - \alpha)\, d\alpha =$$

$$= \sum_{n=-\infty}^{\infty} \int\limits_{-\infty}^{\infty} T f(\alpha)\, \delta(\alpha - nT)\, h(t - \alpha)\, d\alpha =$$

$$= \sum_{n=-\infty}^{\infty} f(nT) \frac{\sin 2\pi W (t - nT)}{2\pi W (t - nT)}. \qquad (3.8)$$

Этот результат обычно называется *теоремой отсчетов*.

К сожалению, большинство представляющих интерес спектральных плотностей мощности не равно нулю вне какого-либо конечного интервала частот. Например, никакой сигнал конечной длительности не может иметь спектр, обладающий этим свойством. Наиболее типичная спектральная плотность мощности показана на рис. 3.3*а*. Однако, хотя может не быть частоты, после которой спектральная плотность обращается в нуль, для любых процессов с конечной мощностью доля общей мощности на частотах $|f| > f_0$, где f_0 — некоторое достаточно большое, но конечное значение, является сколь угодно малой. Представляется разумным в этом слу-

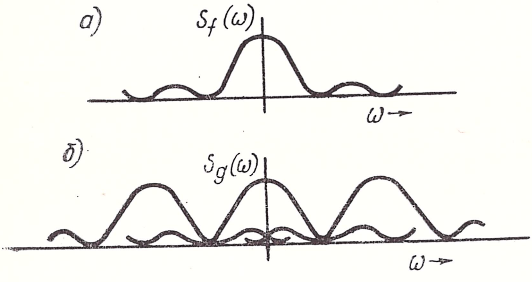


Рис 3.3. Явление «мимикрии частот»: *а)* спектр сигнала; *б)* спектр отсчетов сигнала

чае брать отсчеты функции каждые $T=1/2f_0$ секунд, получая функцию с характерным спектром, показанный на рис. 3.3*б*. Результатом такой процедуры будет «свернутый назад» спектр. Если теперь отфильтровать всю энергию на частотах, больших f_0, то полученный спектр не будет совпадать со спектром первоначального процесса и первоначальный процесс не может быть точно восстановлен по периодическим отсчетам. Ошибка, вызванная этим «сворачиванием назад», часто называется ошибкой «мимикрии частот»; ее легко определить с помощью равенства (3.7). В большинстве практических случаев минимальная приемлемая частота отсчетов ограничивается величиной допустимой ошибки «мимикрии частот».

3.3. О расчете систем импульсной модуляции

Удобной мерой качества аналоговых систем связи является *отношение сигнал/шум*, определяемое следующим образом. Если желаемым сигналом приемника является $s(t)$, а действительным — $y(t)$, то мощность шума, по определению,

$$\sigma_n^2 = \lim_{T\to\infty} \frac{1}{2T} \int_{-T}^{T} [y(t) - s(t)]^2\, dt. \tag{3.9}$$

Мощность сигнала[1], очевидно,

$$\sigma_s^2 = \lim_{T\to\infty} \frac{1}{2T} \int_{-T}^{T} [s(t) - \overline{s(t)}]^2\, dt, \tag{3.10}$$

а отношение сигнал/шум

$$S/N = \sigma_s^2/\sigma_n^2. \tag{3.11}$$

По аналогии определим отношение сигнал/шум в импульсной системе связи как

$$\frac{S}{N} = \frac{\operatorname{var}(s_i)}{E[(s_i - \hat{s}_i)^2]}, \tag{3.12}$$

где s_i — отсчет, который должен быть передан на интервале $iT_s < t < (i+1)\,T_s$, а $\hat{s}_i$ — оценка этого отсчета, выданная на выходе приемника. (Последовательности s_i и $\hat{s}_i$ предполагаются стационарными, так что величина S/N в действительности не зависит от i.) Мерой качества импульсной системы связи будет служить в этой главе отношение сигнал/шум, определенное равенством (3.12). Эквивалентной мерой при заданной дисперсии сигнала является среднеквадратическая ошибка $E[(s_i-\hat{s}_i)^2]$.

---

[1] Средняя амплитуда сигнала $\overline{s(t)} = \lim_{T\to\infty} \frac{1}{2T} \int_{-T}^{T} s(t)\, dt$ в идеале равна нулю. Если $\overline{s(t)}$ не равна нулю, то та же информация, в принципе, может быть передана сигналом $s(t) - \overline{s(t)}$, и поэтому мощность сигнала определяется опять как дисперсия $s(t)$. (*Прим. авт.*).

Одной из мер стоимости достижения некоторого заданного уровня качества является ширина полосы частот модулированного сигнала. Имеется несколько разумных способов численного определения этой меры. Ширина полосы может быть, например, определена как ширина идеального полосового фильтра, необходимая, чтобы пропустить, допустим, 90% мощности сигнала. Эта мера, конечно, делает необходимым определение действительного спектра сигнала.

Второй, часто используемой мерой ширины полосы, занимаемой сигналом, является его *эффективная ширина полосы,* определяемая как обратная величина максимальной плотности (в каналах на единицу ширины полосы частот), с которой каналы, передающие статистически одинаковые сигналы, могут быть уплотнены по частоте без взаимной интерференции. Это означает, что выходной сигнал демодулятора для любого канала должен быть независимым от сигналов, передаваемых по любым другим каналам.

Так как мы будем иметь дело исключительно с импульсными системами связи, то полезно следующее выражение для спектральной плотности мощности случайной последовательности статистически независимых импульсов:

$$S(\omega)=\frac{1}{T_s}\int p(\mu)\,|F_\mu(\mathrm{i}\,\omega)|^2\,d\mu-\frac{1}{T_s}\left|\int p(\mu)\,F_\mu(\mathrm{i}\,\omega)\,d\mu\right|^2+$$

$$+\frac{2\pi}{T_s^2}\sum_{n=-\infty}^{\infty}\left|\int p(\mu)\,F_\mu(\mathrm{i}\,\omega)\,d\mu\right|^2\delta\left(\omega-\frac{2\pi n}{T_s}\right), \qquad (3.13)$$

где $F_\nu(\mathrm{i}\omega)$ — преобразование Фурье временнóй функции $x(t,\ \nu)$. Эта последняя функция определяет переданный сигнал $x(t-iT_s, \nu_i)$ на каждом заданном интервале $iT_s<t<(i+1)\,T_s$ и предполагается равной нулю вне интервала $(0,\ T_s)$, т. е. $F_\nu(\mathrm{i}\,\omega)=\int\limits_0^T x(t,\ \nu)\,\mathrm{e}^{-\mathrm{i}\,\omega\,t}\,dt$; $p(\nu)$ в ф-ле (3.13) — плотность распределения вероятности параметра ν сигнала. Равенство (3.13) справедливо, когда параметры ν_i $(i=\ldots,\ -1,\ 0,\ 1,\ \ldots)$ в передаваемой последовательности являются независимыми и порождаются стационарным источником.

3.4. Оптимальная демодуляция

Оптимальный импульсный демодулятор непрерывного параметра в соответствии с критерием § 3.3 минимизирует среднеквадратическую разность между переданным параметром ν и выходом приемника $\hat{\nu}$. Таким образом, оптимальный демодулятор является формулой оценки параметра в смысле, указанном в § 2.9, со стоимостью ошибки, равной ее среднеквадратической величине. Для того чтобы свести рассматриваемую здесь задачу к дискретному случаю (§ 2.9), пропустим принятый сигнал $y(t)$ через идеальный фильтр нижних частот с полосой B. Профильтрованный сигнал может быть представлен множеством выборок $Y=\{y_i\}=\{y_f(i\Delta t)\}$, $i=1, 2, \ldots, k=2BT_s$ с $\Delta t=1/2B$, где индекс f означает, что функция $y(t)$ была профильтрована до того, как были взяты выборки[1]. Так как принятый сигнал не ограничен какой-либо конечной шириной полосы B, то при фильтрации некоторая информация, конечно, теряется. Вначале определим вид оптимального демодулятора для наблюдаемых Y при некоторой конечной ширине полосы B, а затем при $B \to \infty$. В пределе никакая информация не теряется, и получающийся демодулятор будет оптимальным без всякого ограничения.

Как было показано в гл. 2, оптимальная формула оценки параметра ν, основанная на использовании наблюдаемых Y, когда стоимостная функция представляет собой среднеквадратическую ошибку, является условным средним

$$\hat{\nu}=E(\nu\,|\,Y). \tag{3.14}$$

Чтобы вычислить эту оценку, нужно знать апостериорную плотность распределения вероятности $p(\nu\,|\,Y)$:

$$p(\nu\,|\,Y)=p(Y\,|\,\nu)\,p(\nu)/p(Y), \tag{3.15}$$

где $p(\nu)$ — априорная плотность распределения параметра ν. Записывая $y_i=y_f(i\Delta t)=Ax_f(i\Delta t,\ \nu)+n_f(i\Delta t)\triangleq Ax_i(\nu)+n_i$, где $x_f(t,\nu)$ и $n_f(t)$ представляют собой профильтрованный сигнал и профильтрованный аддитивный шум соответственно, получаем

$$p(\nu\,|\,Y)=K_0\,p\,[n_1=y_1-Ax_1(\nu),\quad n_2=y_2-\\ -Ax_2(\nu),\ldots,\ n_k=y_k-Ax_k(\nu)]\,p(\nu), \tag{3.16}$$

где K_0 — нормировочная постоянная, не зависящая от ν. Более того, так как $n(t)$ — выборочная функция белого гауссовского шума с односторонней спектральной плотностью N_0 Вт/Гц, то $p(n_1, n_2, \ldots, n_k)$ — многомерная гауссовская плотность распределения. Спектр этого шума после его прохождения через идеальный фильтр нижних частот с шириной полосы B имеет следующий вид:

$$S_n(f)=\begin{cases} N_0/2 & \text{при } |f|\leqslant B; \\ 0 & \text{в остальных случаях.}\end{cases} \tag{3.17}$$

Следовательно, автокорреляционная функция

$$R_n(\tau)=N_0B\,\frac{\sin 2\pi B\tau}{2\pi B\tau} \tag{3.18}$$

---

[1] Так как статистики сигнала не зависят от рассматриваемого интервала, то можно без потери общности ограничиться рассмотрением сигнала $y(t)=Ax(t,\mu)+n(t)$ для $0<t<T_s$. *(Прим. авт.)*.

и $R_n(i\Delta t) = R_n(i/2B) = 0$ для $i = 1, 2, \ldots$, а $R_n(0) = N_0 B$. Таким образом,

$$p(n_1, n_2, \ldots, n_k) = \frac{1}{(2\pi N_0 B)^{k/2}} \exp\left[-\frac{1}{2N_0 B}\sum_{i=1}^{k} n_i^2\right]; \tag{3.19}$$

$$p(\nu|Y) = \frac{K_0}{(2\pi N_0 B)^{k/2}} \exp\left[-\frac{1}{2N_0 B}\sum_{i=1}^{k}[y_f(i\Delta t) - Ax_f(i\Delta t, \nu)]^2\right]p(\nu) =$$

$$= K_1 p(\nu) \exp\left\{\frac{1}{N_0 B}\sum_{i=1}^{k}\left[y_f(i\Delta t) A x_f(i\Delta t, \nu) - \frac{A^2}{2} x_f^2(i\Delta t, \nu)\right]\right\}, \tag{3.20}$$

где K_1 также не зависит от ν. Теперь, устремляя $B \to \infty$ $(\Delta t \to 0)$, получим

$$p(\nu|y(t)) = K_1' p(\nu) \exp\left\{\frac{1}{N_0}\int_0^{T_s}[2Ay(t)x(t, \nu) - A^2 x^2(t, \nu)]\,dt\right\}. \tag{3.21}$$

Следовательно, оптимальный демодулятор вычисляет величину

$$\hat{\nu} = \int \nu p(\nu|y(t))\,d\nu, \tag{3.22}$$

где функция $p[\nu|y(t)] \triangleq p(\nu|y(t), 0 \leqslant t \leqslant T_s)$ задается равенством (3.21).

В § 2.9 было замечено, что если $p(\nu|Y)$ — унимодальная симметрическая функция ν, то условное математическое ожидание ν равно условной моде распределения. Таким образом, в этом случае эквивалентной операцией для оптимального демодулятора будет отыскание такой оценки $\hat{\nu}$, для которой апостериорная плотность распределения $p[\hat{\nu}|y(t)]$ достигает своего максимума.

Если априорная плотность вероятности $p(\nu)$ не известна, то могут оказаться пригодными другие формулы оценок, например, *минимаксная* формула оценки и формула оценки *максимального правдоподобия* (ср. с § 2.9). На самом деле оценка максимального правдоподобия эффективна, если эффективная оценка существует. В последнем случае она становится оптимальной оценкой в среднеквадратическом смысле, если вводится дополнительное ограничение, чтобы оценка была несмещенной. Даже если эффективная оценка не существует, оценка максимального правдоподобия часто имеет небольшое смещение, а дисперсия не на много превышает теоретический минимум, который задается (2.66). Таким образом, ее можно предпочесть в качестве оценки даже, когда известна априорная плотность $p(\nu)$.

Невольно может возникнуть мысль, что оценка максимального правдоподобия всегда будет эффективной в рассматриваемых здесь условиях, так как число k независимых наблюдаемых y_i, на которых основывается каждая оценка, стремится к бесконечности при стремлении к бесконечности ширины полосы B и, как показано в § 2.9, формулы оценок максимального правдоподобия являются асимптотически эффективными. К сожалению, дисперсии N_0B этих наблюдаемых одновременно стремятся к бесконечности, а в утверждении § 2.9 предполагается, напротив, что статистики не независят от k. Асимптотические свойства формул оценок максимального правдоподобия проявляются, однако, когда отношение сигнал/шум «на входе» $R=A^2T_s/N_0$ достаточно велико (это будет показано в дальнейшем). Здесь T_s — непосредственный аналог числа независимых выборок, когда наблюдаемые дискретны.

Формула оценки максимального правдоподобия имеет и другое преимущество по сравнению с большинством других формул оценок; как будет вскоре показано, ее часто легче реализовать. По этим двум причинам формулы оценок максимального правдоподобия (или принципа максимума правдоподобия) образуют класс формул оценок, который наиболее широко применяется для демодуляции.

Оценка максимального правдоподобия $\hat{\nu}$ параметра ν, по определению, является решением уравнения правдоподобия

$$\frac{\partial}{\partial \nu}\log p\,[y(t)\,|\,\nu] = \frac{\dfrac{\partial}{\partial \nu}\,p\,[y(t)\,|\,\nu]}{p\,[y(t)\,|\,\nu]} = 0.$$

Используя байесовское правило и равенство (3.21), получаем, что оценка максимального правдоподобия представляет собой решение уравнения

$$\frac{\partial}{\partial \nu}\log p\,[y(t)\,|\,\nu] = \frac{2A}{N_0}\int\limits_0^{T_s}[y(t) - Ax(t,\ \nu)]\,\frac{\partial x(t,\ \nu)}{\partial \nu}\,dt = 0. \qquad (3.23)$$

Безотносительно к используемому критерию все оптимальные формулы оценок имеют одно и то же важное свойство; принятый сигнал входит в них лишь через посредство взаимокорреляционных коэффициентов вида

$$\int\limits_0^{T_s} y(t)\,z(t,\ \nu)\,dt, \qquad (3.24)$$

где для примера $z(t,\ \nu)=x(t,\ \nu)$ [см. равенство (3.21)] или $z(t,\ \nu)=\partial x(t,\ \nu)/\partial\nu$ [см. равенство (3.23)]. Один из способов определения этих коэффициентов состоит в пропускании принятого сигнала через фильтр, имеющий импульсный отклик:

$$h(t) = \begin{cases} z(T_s - t,\ \nu) & \text{при } 0 < t < T_s; \\ 0 & \text{в остальных случаях.} \end{cases} \qquad (3.25)$$

Такой фильтр называется *согласованным фильтром* (он «согласован» с сигналом $z(t,\ \nu)$). Всегда можно, конечно, построить согласованный фильтр, как *взаимный коррелятор,* т. е. с помощью умножения $y(t)$ на $z(t, \nu)$ и интегрирования, как показано на рис. 3.4*а*.

Часто $z(t, \nu)$ имеет вид $z(t, \nu)=s(t, \nu)\sqrt{2}\sin(\omega_c t+\Phi)$, где множитель $\sqrt{2}\sin(\omega_c t+\Phi)$ представляет собой несущую. Обычно более практичным в этом случае является демодулятор, изображенный на рис. 3.4*б*. Единственное различие между этим устройством и коррелятором рис. 3.4*а* состоит во включении фильтра нижних частот. Если частота $\omega_c/2\pi$ велика по сравнению с максимальной существенной частотной компонентой $s(t, \nu)$, то выход первого умножителя состоит из двух относительно узкополосных составляющих: одной, сконцентрированной около нулевой частоты, и другой — около частоты $2\omega_c/2\pi$. В силу того, что система умножитель-интегратор действует как фильтр с импульсным откликом $h(t)=s(T_s-t, \nu)$, она также представляет собой фильтр, согласованный с низкочастотным сигналом $s(t, \nu)$. Как таковой, он является фильтром нижних частот с шириной полосы, равной ширине полосы сигнала и, следовательно, малой по сравнению с $2\omega_c/2\pi$. Если первый фильтр имеет большую ширину полосы по отношению к полосе согласованного фильтра, то он не оказывает значительного влияния на выход последнего фильтра и демодуляторы на рис. 3.4*а, б* фактически эквивалентны. Однако если ширина полосы этого первого фильтра мала по сравнению с $2\omega_c/2\pi$, то это приводит к устранению составляющих с удвоенными частотами после первой операции умножения. В условиях, принятых здесь, следовательно, не существенно, учитываем ли мы несущую при анализе изучаемых систем связи или нет, поскольку мы вводим в приемник демодулятор, в котором предусмотрено умножение на сигнал несущей.

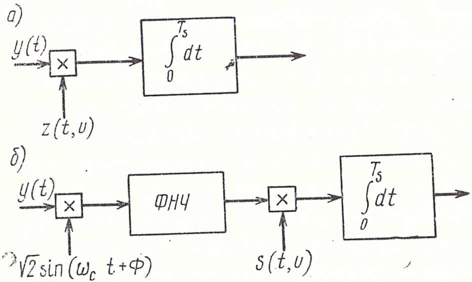


Рис. 3.4. Схемы согласованных фильтров: *а)* реализация взаимного коррелятора; *б)* взаимный коррелятор для модулированной несущей

В общем случае требуется континуум согласованных фильтров, по одному для каждого возможного значения ν безотносительно к тому, как они реализуются. Для того чтобы демодулятор имел какую-либо практическую ценность, нужно, конечно, снизить число этих устройств до некоторого конечного числа. В некоторых случаях это означает, что нужно использовать приближенно оптимальный демодулятор. К счастью, как будет вскоре показано, оптимальные демодуляторы для систем модуляции, рассматриваемых в этой главе, имеют только один или два таких согласованных фильтра.

В заключение параграфа следует упомянуть, что принятый сигнал может содержать другие неизвестные параметры, такие, как амплитуда сигнала или фаза несущей. Если можно предположить, что эти параметры остаются постоянными в течение всего времени передачи, то их, вообще говоря, можно оценить (как указано в § 2.9) с достаточной точностью, что позволит обращаться с ними как с известными. В другом крайнем случае, когда можно предположить, что они принимают независимые значения на каждом T_s-секундном интервале, их можно оценить одновременно с каждым информационным параметром ν_i, хотя сами по себе они не несут информации. В том случае, когда известны априорные распределения этих «мешающих» параметров, оценки информационных параметров иногда можно усреднить по этим величинам, что избавляет от необходимости их явной оценки. А именно, обозначая неизвестные параметры вектором $\mathbf{\Phi}$, вначале определяем функцию $p[y(t)\,|\,\nu,\ \mathbf{\Phi}]$ или $p[\nu\,|\,y(t),\ \mathbf{\Phi}]$, или $E[\nu\,|\,y(t),\ \mathbf{\Phi}]$, а затем усредняем ее по неизвестным параметрам $\mathbf{\Phi}$, получая в результате

$$p\,[y\,(t)|\nu] = \int\limits_{-\infty}^{\infty} p\,[y\,(t)|\nu,\ \mathbf{\Phi}]\,p\,(\mathbf{\Phi}|\nu)\,d\,\mathbf{\Phi}$$

(ср. с § 2.4). Частный пример впервые рассматривается в § 3.6.

3.5. Когерентная амплитудно-импульсная модуляция

Огибающая амплитудно-импульсномодулированного сигнала представляет собой последовательность импульсов фиксированной длительности, равной T_s секунд; амплитуды импульсов меняются в соответствии с передаваемой информацией ν_i. Если огибающие импульсов прямоугольны, то передаваемый сигнал

$$x\,(t - iT_s,\ \nu_i) = \sqrt{2}\,\nu_i \sin \omega_c t, \quad iT_s < t < (i+1)\,T_s. \tag{3.26}$$

Чтобы сохранить независимость сигнала от длины интервала, потребуем, чтобы $\omega_c = \pi r/T_s$, где r — либо целое число, либо число, много большее единицы.

Пусть $y(t)$ обозначает сумму принятого сигнала и шума:

$$y\,(t) = Ax\,(t,\ \nu) + n\,(t) = \sqrt{2}\,A\,\nu \sin \omega_c t + n\,(t), \quad 0 < t < T_s. \tag{3.27}$$

Из равенства (3.21) находим, что апостериорная плотность распределения величины ν при заданном $y(t)$ $0 < t < T_s$, имеет вид

$$\begin{aligned} p\,[\nu|y\,(t)] &= Kp\,(\nu) \exp\left\{\frac{2A}{N_0}\int\limits_0^{T_s} y\,(t)\left(\sqrt{2}\,\nu \sin \omega_c t\right) dt - \nu^2 \frac{\mathcal{E}}{N_0}\right\} = \\ &= Kp\,(\nu) \exp\left\{2R\left(\nu I - \frac{\nu^2}{2}\right)\right\}, \end{aligned} \tag{3.28}$$

где K — нормирующая постоянная, не зависящая от ν; величина $\mathcal{E} = A^2 T_s$ представляет собой энергию принятого импульса, если

$\nu=1$; $R=\mathcal{E}/N_0$ и $I=(1/AT_s)\int\limits_0^{T_s} y(t)\sqrt{2}\sin\omega_c t dt$. Если случайная величина ν имеет равномерное распределение

$$p(\nu)=\begin{cases}\dfrac{1}{2a} & \text{при } -a\leqslant\nu\leqslant a;\\ 0 & \text{в остальных случаях,}\end{cases} \tag{3.29}$$

то

$$\frac{\partial p[\nu|y(t)]}{\partial\nu}=\left[2R(I-\nu)+\frac{1}{p(\nu)}\frac{dp(\nu)}{d\nu}\right]p[\nu|y(t)] \tag{3.30}$$

и $p[\nu|y(t)]$ — унимодальная функция ν с модой $\nu=\hat{\nu}$, где

$$\hat{\nu}=\begin{cases}I & \text{при } -a\leqslant I\leqslant a;\\ -a & \text{при } I<-a;\\ a & \text{при } I>a.\end{cases} \tag{3.31}$$

Формула оценки по максимуму апостериорной вероятности случайной величины ν совпадает, следовательно, с величиной $\hat{\nu}$, определенной равенством (3.31). (Заметим, что $p[\nu|y(t)]$ — несимметричная функция ν, кроме случая, когда $I=0$, и $\hat{\nu}$ в общем случае не является оптимальной оценкой величины ν в среднеквадратическом смысле.)

Оценка максимального правдоподобия $\hat{\nu}$ согласно равенству (3.23) совпадает с решением уравнения

$$\frac{\partial\log p[y(t)|\nu]}{\partial\nu}=\frac{2A}{N_0}\int\limits_0^{T_s}[y(t)-\sqrt{2}A\nu\sin\omega_c t]\sqrt{2}\sin\omega_c t dt=0, \tag{3.32}$$

и решение в этом случае является единственным для всех I:

$$\hat{\nu}=I=\frac{1}{AT_s}\int\limits_0^{T_s}\sqrt{2}\,y(t)\sin\omega_c t dt. \tag{3.33}$$

Независимо от того, какая из этих формул оценок используется, демодулятор имеет вид, изображенный на рис. 3.5. Устройство, производящее оценку, может быть весьма простым (просто короткое замыкание в случае оценки максимального правдоподобия) или относительно сложным (как в случае формулы оценки $\hat{\nu}=E[\nu|y(t)]=K\int\nu p(\nu)\exp\{2R(\nu I-(\nu^2/2))\}d\nu$.

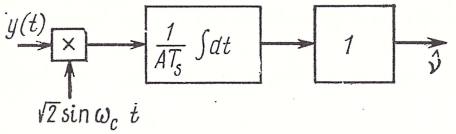


Рис. 3.5. Функциональная схема демодулятора когерентной по фазе АИМ:
1 — устройство, производящее оценку

Хотя нетрудно определить отношение сигнал/шум на выходе любого из этих демодуляторов, вычислим его только для демодулятора максимального правдоподобия, для которого оно принимает особенно простой вид. Так как шум гауссовский, то оценка максимального правдоподобия $\hat{v}$ величины v [см. ф-лу (3.33)] имеет гауссовское распределение с условным средним

$$E(\hat{v}|v) = E\left\{v + \frac{\sqrt{2}}{AT_s}\int_0^{T_s} n(t)\sin\omega_c t dt|v\right\} = v \tag{3.34}$$

и, следовательно, является несмещенной. Условная среднеквадратическая ошибка имеет вид

$$\sigma_n^2 = E[(\hat{v} - v)^2|v] = E\left\{\frac{2}{A^2T_s^2}\int_0^{T_s}\int_0^{T_s} n(t)n(u)\sin\omega_c t\sin\omega_c u du dt\right\} = \frac{1}{2R} \tag{3.35}$$

и не зависит от v. Так как

$$E\left[\frac{\partial\log p[y(t)|v]}{\partial v}\,\Big|\,v\right]^2 = E[2R(\hat{v} - v)|v]^2 = 2R, \tag{3.36}$$

то оценка максимального правдоподобия величины v эффективна (см. § 2.9). Наконец, отношение сигнал/шум на выходе просто равно

$$\frac{S}{N} = \frac{\sigma_s^2}{\sigma_n^2} = \frac{2\bar{\mathcal{E}}}{N_0}, \tag{3.37}$$

где $\bar{\mathcal{E}} = E(v^2)\,\mathcal{E}$ — средняя энергия принятого сигнала.

Для сравнения рассмотрим теперь оптимальные демодуляторы, если амплитуда сигнала имеет гауссовское распределение

$$p(v) = \frac{1}{\sqrt{2\pi}\,\sigma_s} e^{-v^2/2\sigma_s^2}. \tag{3.38}$$

В этом случае

$$p[v|y(t)] = K\exp\left\{2RvI - \left(R + \frac{1}{2\sigma_s^2}\right)v^2\right\} =$$

$$= K'\exp\left\{-\left(R + \frac{1}{2\sigma_s^2}\right)(v - \hat{v})^2\right\}, \tag{3.39}$$

где $\hat{v} = I/[1 + (1/2R\sigma^2{}_s)]$. Следовательно, $p[v\,|\,y(t)]$ — также гауссовская плотность распределения, и она симметрична и унимодальна. Поэтому как оптимальная среднеквадратическая оценка, так и оценка по максимуму апостериорной вероятности величины v имеет вид

$$\hat{v} = E[v|y(t)] = \frac{I}{1 + \dfrac{1}{2R\sigma_s^2}} = \frac{I}{1 + \left(\dfrac{2\mathcal{E}}{N_0}\right)^{-1}}, \tag{3.40}$$

где вновь $\overline{\mathcal{E}} = \mathcal{E}\sigma^2_s$ — средняя энергия принятого сигнала. Более того,

$$\sigma_n^2 = E(\hat{\nu}-\nu)^2 = 1/(2R + 1/\sigma_s^2), \tag{3.41}$$

так что

$$S/N = \sigma_s^2/\sigma_n^2 = 1 + 2\overline{\mathcal{E}}/N_0. \tag{3.42}$$

В противоположность этому формула оценки максимального правдоподобия, которая не зависит от априорного распределения, остается такой же, как ранее, и приводит к отношению сигнал/шум (3.37). Оценка максимального правдоподобия, как уже отмечалось, является несмещенной. Оценка, дающая минимум среднеквадратической ошибки (3.40), однако, имеет смещение при любом конечном отношении сигнал/шум $\overline{\mathcal{E}}/N_0$:

$$E(\hat{\nu}|\nu) = \frac{E(I|\nu)}{1+(2\overline{\mathcal{E}}/N_0)^{-1}} = \frac{\nu}{1+(2\overline{\mathcal{E}}/N_0)^{-1}}. \tag{3.43}$$

С помощью ф-лы (3.13) можно легко найти спектр и, следовательно, ширину полосы АИМ сигнала. Ограничимся здесь, однако, рассмотрением (имеющим скорее теоретический, чем практический интерес) меры ширины полосы — *эффективной ширины полосы*, введенной в § 3.3. Напомним, что эта мера определяется максимальной возможной плотностью, с которой АИМ каналы могут быть уплотнены по частоте без взаимной интерференции. Чтобы определить ее, рассмотрим идеальную ситуацию, в которой все каналы имеют совершенную синхронизацию; l-й канал передает сигнал вида $\sqrt{2}\,x_l \sin\omega_l t$, где x_l постоянно на каждом интервале $iT_s < t < (i+1)T_s$ для всех l. Тогда выход детектора m-го канала, вызванный импульсом, переданным по l-му каналу,

$$\frac{2}{T_s} x_l \int_0^{T_s} \sin\omega_l t \sin\omega_m t\,dt = 0,\quad l \neq m,$$

если ω_l и ω_m — целые, кратные величине πT_s. Так как два смежных канала должны быть разделены по частоте хотя бы интервалом $1/2T_s$ герц, то эффективная ширина полосы канала, очевидно, равна $B_{\text{эфф}} = 1/2T_s$ герц.

3.6. Некогерентная по фазе амплитудно-импульсная модуляция

Считается, что в некогерентной системе связи фаза Φ несущей является случайной величиной, равномерно распределенной на интервале $(0,2\pi)$, и не делается никаких попыток оценить ее истинное значение. Некогерентная передача ведется тогда, когда практически неразумно оценивать Φ непосредственно. Такая ситуация может возникнуть либо из-за ограничений на сложность оборудования, либо потому, что Ф изменяется слишком быстро вследствие нестабильности генератора, что не позволяет сделать точную оценку. В любом случае, если Ф — медленно меняющаяся функция времени на интервале T_s, то разумно (удобно) рассматривать ее как равномерно распределенную случайную величину, постоянную на любом интервале передачи одного импульса. Более того, если T_s много больше, чем период несущей $2\pi/\omega_c$, то не будет противоречия в предположениях (которые будут сделаны в этом параграфе), что фаза несущей неизвестна, а фаза огибающей известна точно.

Если необходимо произвести некогерентную обработку, то передаваемый сигнал должен быть изменен, чтобы отразить тот факт, что знак величины ν определить нельзя. Не существует способа определить, была ли амплитуда равна ν, а фаза несущей Ф или же амплитуда была $-\nu$, а фаза несущей $\pi+\Phi$. По этой причине, если демодулятор должен быть некогерентным, обычно ограничиваются только положительными значениями величины ν. Действительный сигнал s по предположению опять имеет нулевое среднее; поэтому ν имеет вид $s+a$, например, когда $p(s)=1/2a$, $-a<s<a$.

С этой оговоркой передаваемый сигнал будет таким же, как и ранее [ср. с ф-лой (3.27)], но теперь (при рассмотрении задач, связанных с анализом характеристик демодулятора) принимаемый сигнал имеет вид $x(t,\ \nu,\ \Phi)=\sqrt{2}\nu\sin(\omega_c t+\Phi)$ и является функцией двух случайных параметров, лишь один из которых следует оценить. Следовательно, необходимо видоизменить выводы § 3.4, чтобы принять во внимание этот факт. Начнем с замечания, что оптимальный демодулятор сигнала $y(t)=Ax(t,\ \nu,\ \Phi)+n(t)$, когда фаза несущей известна, основывается на использовании плотности распределения [см. ф-лу (3.21)]:

$$p\,[\nu|y(t),\ \Phi]=K'\exp\left[\frac{2R\,\nu}{AT_s}\int\limits_0^{T_s} y\,(t)\sqrt{2}\sin\,(\omega_c t+\Phi)\,dt-R\,\nu^2\right]p\,(\nu|\Phi)=$$

$$=K'p\,(\nu)\exp\{-R\,\nu^2+2R\,\nu\,[X\cos\Phi+Y\sin\Phi]\},\qquad(3.44)$$

где $$X=\frac{1}{AT_s}\int\limits_0^{T_s} y\,(t)\sqrt{2}\sin\omega_c\,t dt;$$

$$Y=\frac{1}{AT_s}\int\limits_0^{T_s} y\,(t)\sqrt{2}\cos\omega_c\,t dt$$

и предполагается, что ν не зависит от Ф. Безусловная апостериорная плотность распределения вероятности $p[\nu\,|\,y(t)]$, следовательно, имеет вид

$$p\,[\nu|y\,(t)]=\int\limits_0^{2\pi} p\,[\nu|y\,(t),\ \Phi]\,p\,[\Phi|y\,(t)]\,d\,\Phi=$$

$$=Kp(\nu)\int\limits_0^{2\pi} p(\Phi)\exp\{-R\,\nu^2+2R\,\nu\,M\cos(\theta-\Phi)\}\,d\,\Phi, \qquad (3.45)$$

где $M^2=X^2+Y^2$ и $\theta=\mathrm{arctg}[Y/X]$. Если $p(\Phi)=\frac{1}{2\pi}$, $0<\Phi<\pi$, то

$$p[\nu|y(t)]=Kp(\nu)\exp\{-R\,\nu^2\}\frac{1}{2\pi}\int\limits_0^{2\pi}\exp\{2RM\,\nu\cos(\theta-\Phi)\}\,d\,\Phi=$$

$$=Kp(\nu)\exp\{-R\,\nu^2\}\,I_0(2RM\,\nu), \qquad (3.46)$$

где $I_n(x)$ — модифицированная функция Бесселя n-го порядка первого рода.

Так как величина ν не может быть отрицательной, то $p[\nu\,|\,y(t)]$ не будет симметричной функцией ν независимо от вида функции $p(\nu)$. Таким образом, оценка, оптимальная в смысле среднеквадратической ошибки, максимальная апостериорная оценка и оценка максимального правдоподобия в общем случае будут различны. Рассмотрим здесь только последнюю оценку. Оценкой максимума правдоподобия величины ν является решение уравнения

$$\frac{\partial\log p\,[y\,(t)|\nu]}{\partial\,\nu}=2R\left(M\,\frac{I_1\,(2RM\,\nu)}{I_0\,(2RM\,\nu)}-\nu\right)=0, \qquad (3.47)$$

и, следовательно, оценка имеет вид [1]

$$\hat{\nu}=MI_1(2RM\,\hat{\nu})/I_0(2RM\,\hat{\nu}). \qquad (3.48)$$

Имеется несколько трудностей, связанных с этим результатом. Во-первых, то, что оценка величины ν является решением трансцендентного уравнения, по меньшей мере, является неудобным. Более того, решение зависит от отношения сигнал/шум $R=\mathcal{E}/N_0$, которое, следовательно, должно быть известным или должно быть оценено.

В отсутствии шума, когда $R\to\infty$, имеем $I_1(2RM\nu)/I_0(2RM\nu)\to 1$, и оценка максимального правдоподобия величины ν

$$\hat{\nu}=M. \qquad (3.49)$$

Хотя эта оценка не является оптимальной для любого уровня шумов, она тем не менее имеет смысл даже тогда, когда отношение сигнал/шум не очень велико, и часто удобно использовать ее вместо оценки максимального правдоподобия. Функциональная схема этой аппроксимации некогерентного по фазе АИМ приемника максимального правдоподобия показана на рис. 3.6 [2].

Интересно, что равенство (3.49) в точности описывает оценку, которая получилась бы, если бы одновременно оценивались амплитуда и фаза принятого сигнала. Оценка максимального правдоподобия величины ν при заданной Φ [ф-лу (3.23)] удовлетворяет уравнению

---

[1] Это уравнение имеет также решение $\nu=0$, которое отбрасывается, так как оно не зависит от принятого сигнала. *(Прим. авт.)*.

[2] Другая реализация рассмотрена в § 4.3. *(Прим. авт.)*.

$$\frac{\partial \log p\,[y(t)|\nu,\ \Phi]}{\partial \nu} = 2R\,[X\cos\Phi + Y\sin\Phi - \nu] = 0 \tag{3.50}$$

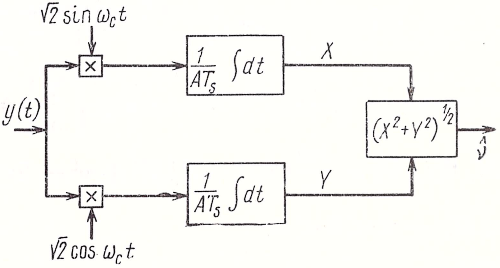


Рис. 3.6. Функциональная схема демодулятора некогерентной по фазе АИМ

а оценка максимального правдоподобия величины Φ должна быть решением уравнения

$$\frac{\partial \log p\,[y(t)|\nu,\ \Phi]}{\partial \Phi} = 2R\,\nu\,[Y\cos\Phi - X\sin\Phi] = 0. \tag{3.51}$$

Решая одновременно оба эти уравнения, находим совместные формулы оценок максимального правдоподобия для пары неизвестных параметров ν и Φ:

$$\hat{\Phi} = \theta = \operatorname{arc\,tg}\left[\frac{Y}{X}\right]; \tag{3.52}$$

$$\hat{\nu} = M = [X^2 + Y^2]^{1/2}. \tag{3.53}$$

(Это решение не единственно. Другое решение, определяемое равенствами $\hat{\nu}=0$ и $\hat{\Phi}=-\operatorname{arctg}[X/Y]$, дает оценку амплитуды, которая не зависит от принятого сигнала, и поэтому отбрасывается.)

Хотя при некогерентном приеме оценка Φ не производится, ее можно построить по тем же наблюдаемым, которые используются для оценки величины ν. В силу того что по предположению фаза Φ считается медленно меняющейся во времени (схема приемника, описанная здесь, может быть использована только при этом предположении), $\hat{\Phi}_i$ — оценка i-го импульса — должна нести некоторую информацию относительно фазы $(i+1)$-го импульса. Таким образом, в принципе, некогерентный АИМ прием может быть улучшен при использовании оценок фаз, которые можно, вообще говоря, получить лишь с чуть большими усилиями.

Чтобы определить среднее и дисперсию оценки $\hat{\nu}=M$, заметим, что, когда $y(t)=\sqrt{2}A\,\nu\sin(\omega_c t+\Phi)+n(t)$, то X и Y имеют совместное гауссовское распределение, причем

$E(X) = \nu\cos\Phi,\quad E(Y) = \nu\sin\Phi;$

$$\sigma_n^2 = E(X^2) - E^2(X) = E(Y^2) - E^2(Y) = \frac{1}{2R}\,; \tag{3.54}$$

$$E(XY) - E(X)\,E(Y) = 0.$$

Таким образом,

$$p(X,\, Y|\nu,\, \Phi) = \frac{1}{2\pi\sigma_n^2}\exp\left\{-\frac{(X-\nu\cos\Phi)^2 + (Y-\nu\sin\Phi)^2}{2\sigma_n^2}\right\} \tag{3.55}$$

и, полагая $(X^2+Y^2)^{1/2} = M$ и $\operatorname{arctg}\left[\frac{Y}{X}\right] = \Phi$, получаем

$$p(M,\, \theta|\nu,\, \Phi) = \frac{MR}{\pi}\exp\{-R\,[M^2+\nu^2-2\nu M\cos(\theta-\Phi)]\},$$

$$0 < M,\quad -\pi < \theta < \pi. \tag{3.56}$$

Тогда

$$p(M|\nu,\, \Phi) = \int_{-\pi}^{\pi} p\,(M,\, \theta|\Phi,\, \nu)\, d\theta = 2RM\exp\{-R\,[M^2+\nu^2]\}\times$$

$$\times I_0(2MR\nu) = p\,(M \mid \nu),\quad 0 < M, \tag{3.57}$$

и это выражение не зависит от Φ. Далее

$$E\,(M \mid \nu) = \int_0^\infty Mp\,(M \mid \nu)\, dM =$$

$$= \frac{\sqrt{\pi}}{2R^{1/2}}\, e^{-R\nu^2/2}\left[(1+R\nu^2)\, I_0\left(\frac{R\nu^2}{2}\right) + R\nu^2 I_1\left(\frac{R\nu^2}{2}\right)\right];$$

$$E\,(M^2 \mid \nu) = \int_0^\infty M^2 p\,(M \mid \nu)\, dM = \frac{1}{R}(1+R\nu)^2. \tag{3.58}$$

Используя асимптотическое разложение функции

$$I_n(x) = \frac{e^x}{(2\pi x)^{1/2}}\sum_{k=0}^{\infty}\frac{(-1)^k\,\Gamma(n+k+1/2)}{k!\,\Gamma(n-k+1/2)\,(2x)^k}\,,$$

получаем $E(M \mid \nu) = \nu + \frac{1}{4R\nu} + 0\left(\frac{1}{R^2\nu^2}\right)$ и

$$E\,(M^2 \mid \nu) - E^2(M \mid \nu) = \frac{1}{2R} + 0\left(\frac{1}{R^2\nu^2}\right). \tag{3.59}$$

Следовательно, при больших отношениях сигнал/шум R эта оценка является несмещенной для любой амплитуды $\nu \neq 0$ и имеет дисперсию, которая стремится к дисперсии для случая когерентной обработки. Кроме того, так как для любой амплитуды ν имеем

$$E = \left\{\left(\frac{\partial}{\partial\nu}\log p\,[y(t) \mid \nu,\, \Phi]\right)^2\right\} = 4R^2E\,[X\cos\Phi + Y\sin\Phi - \nu]^2 = 2R$$

[ср. с ф-лами (3.50), (3.51)], то дисперсия оценки асимптотически приближается к минимальной возможной дисперсии, определяемой ф-лой (2.66). Таким образом, оценка $\nu = \hat{M}$ асимптотически эффективна. Как отмечено ранее, параметр сигнала ν должен иметь некоторое ненулевое среднее значение $\overline{\nu}$, если демодулятор некогерентен по фазе. В частности, если ν равномерно распределена на интервале $(0, 2a)$, то $\overline{\mathcal{E}} \triangleq \mathcal{E} E(\nu^2) = 4a^2 \mathcal{E}/3$ и отношение сигнал/шум при некогерентной по фазе АИМ в случае больших $\overline{\mathcal{E}}/N_0$ приближенно равно

$$\left(\frac{S}{N}\right)_{\substack{\text{неког.}\\ \text{АИМ}}} \approx \frac{\overline{\mathcal{E}}}{2N_0} = \frac{1}{4}\left(\frac{S}{N}\right)_{\substack{\text{ког.}\\ \text{АИМ}}} \tag{3.60}$$

[ср. с ф-лой (3.37)].

Эффективная ширина полосы для некогерентной АИМ оценивается также, как и в когерентном случае, с помощью определения минимального разделения между каналами, которое устраняет взаимную интерференцию. Однако в случае некогерентного приема на приемнике не известна фаза переданного сигнала. Выходной сигнал приемника для m-го канала, вызванный импульсом, переданным по l-му каналу, равен $(X^2 + Y^2)^{1/2}$, где

$$X \sim \int_0^{T_s} \sin(\omega_l t + \Phi) \sin \omega_m t dt. \text{ и } Y \sim \int_0^{T_s} \sin(\omega_l t + \Phi) \cos \omega_m t dt.$$

Чтобы обе величины X и Y были равны нулю, разность $\omega_l - \omega_m$ должна равняться $2\pi k/T_s$, где k — целое число и эффективная ширина полосы при этом будет $1/T_s$, что вдвое больше, чем при когерентной АИМ.

3.7. Фазовая манипуляция

Если в соответствии с (дискретной по времени) информацией меняется не амплитуда, а фаза несущей, то процесс называется фазовой манипуляцией (или фазовой телеграфией, сокращенно ФТ [1]). Принимаемый сигнал имеет вид:

$$y(t) = Ax(t, \nu) + n(t) = \sqrt{2} A \sin(\omega_c t + \Phi_i) + n(t); \; iT_s < t < (i+1) T_s, \tag{3.61}$$

---

[1] Рассматриваемую в § 3.7 передачу чаще называют фазовой модуляцией, оставляя термин ФТ для случая дискретного множества $\{\Phi_i\}$ (см. § 4.5). Однако в английском оригинале для обоих случаев используется единый термин «phase shift Keying», поэтому при переводе был также сохранен единый термин ФТ. *(Прим. перев.)*.

где величина Φ_i $(-\pi<\Phi_i<\pi)$ представляет собой сигнал, т. е. $\Phi_i=s_i\pi/a$, где $s_i(-a<s_i<a)$ — выборка, которая должна быть передана на i-м импульсном интервале. Как и в случае когерентной АИМ, частота ω_c предполагается равной $r\pi/T_s$, где r — либо целое число, либо число, много большее единицы.

Апостериорная плотность распределения Φ при заданном $y(t)$, $0\leqslant t\leqslant T_s$, согласно § 3.4 имеет вид

$$p[\Phi \mid y(t)] = Kp(\Phi)\exp\left\{\frac{2A}{N_0}\int\limits_0^{T_s} y(t)\sqrt{2}\sin(\omega_c t+\Phi)\,dt\right\} =$$

$$= Kp(\Phi)\exp\{2R(X\cos\Phi + Y\sin\Phi)\}, \tag{3.62}$$

где K — постоянная, не зависящая от Φ; $R=\mathcal{E}/N_0$. Величины X и Y определены в предыдущем параграфе:

$$X=\frac{1}{AT_s}\int\limits_0^{T_s} y(t)\sqrt{2}\sin\omega_c t\,dt;\quad Y=\frac{1}{AT_s}\int\limits_0^{T_s} y(t)\sqrt{2}\cos\omega_c t\,dt.$$

Плотность распределения, очевидно, несимметричная функция Φ, кроме некоторых частных случаев специального выбора величин X и Y; это утверждение справедливо независимо от априорного распределения Φ. Среднее и мода плотности $p[\Phi|y(t)]$ обычно не равны друг другу, так что оптимальная среднеквадратическая оценка и оценка по максимуму апостериорной вероятности не эквивалентны.

Если выборки сигнала распределены равномерно, то $p(\Phi)=1/2\pi$; $-\pi<\Phi<\pi$, и

$$\frac{\partial p[\Phi \mid y(t)]}{\partial\Phi} = 2R[-X\sin\Phi + Y\cos\Phi]\,p[\Phi \mid y(t)]. \tag{3.63}$$

Оценка по максимуму апостериорной вероятности величины Φ, следовательно, имеет вид $\hat{\Phi}=\theta=\operatorname{arctg}(Y/X)$. (Эта оценка однозначна в интервале $-\pi<\Phi<\pi$, если знаки выражений X и Y запоминаются и используются для определения фазового квадранта.) Эта же оценка является оценкой максимального правдоподобия

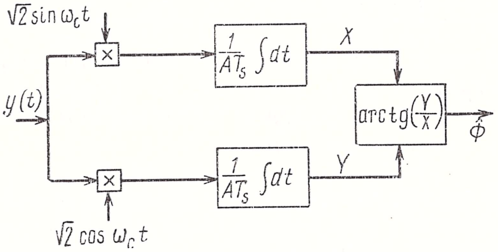


Рис. 3.7. Функциональная схема демодулятора максимального правдоподобия для ФТ

величины Φ_i [ср. с ф-лой (3.51) при $\nu=1$][1]). Получающийся в результате демодулятор изображен на рис. 3.7.

В оптимальном ФТ приемнике используются, таким образом, те же самые решающие переменные X и Y, что и в некогерентном АИМ приемнике, рассмотренном в § 3.6. Там было показано, что если $y(t)=\sqrt{2}\,\nu A\sin(\omega_c t+\Phi)+n(t)$, то

$$p(M,\theta\mid\Phi,\ \nu)=\frac{M}{\pi}R\exp\{-R[M^2+\nu^2-2\nu M\cos(\theta-\Phi)]\};$$

$$0<M,\quad -\pi<\theta<\pi, \tag{3.64}$$

где $M=(X^2+Y^2)^{1/2}$ и $\theta=\operatorname{arctg}(Y/X)$. Здесь величина $\nu=1$ является постоянной, и представляет интерес распределение оценки $\theta=\hat{\Phi}$. Имеем

$$p(\hat{\Phi})=\int\limits_0^\infty p(M,\ \hat{\Phi})\,dM=\frac{R}{\pi}\int\limits_0^\infty M\exp\{-R[M^2+1-2M\cos\theta_e]\}dM=$$

$$=\frac{e^{-R}}{2\pi}+\left(\frac{R}{\pi}\right)^{1/2}\cos\theta_e\, e^{-R\sin^2\theta_e}\frac{1}{\sqrt{2\pi}}\int\limits_0^{(2R)^{1/2}\cos\theta_e}e^{-x^2/2}\,dx=p(\theta_e), \tag{3.65}$$

где $\quad\theta_e=\hat{\Phi}-\Phi;\quad -2\pi\leqslant\theta_e\leqslant 2\pi.$

Вследствие того, что плотность распределения ошибки θ_e оценки величины Φ симметрична относительно $\theta_e=0$, математическое ожидание величины этой ошибки равно нулю и оценка не смещена.

---

[1]) Оптимальную среднеквадратическую оценку также легко найти с помощью разложения Φ в ряд Фурье:

$\Phi=\sum\limits_{n=1}^{\infty}\frac{2}{n}(-1)^{n+1}\sin n\Phi;\ -\pi<\Phi<\pi.$ Таким образом, $E[\Phi\mid y(t)]=$

$$=\frac{K}{2\pi}\sum_{n=1}^{\infty}\frac{2}{n}(-1)^{n+1}\int\limits_{-\pi}^{\pi}\exp\{2RM\cos(\Phi-\theta)\}\sin n\Phi\,d\Phi=K\sum_{n=1}^{\infty}\frac{2}{n}\times$$

$\times(-1)^{n+1}\sin n\theta\, I_n(2RM)$, где $M=(X^2+Y^2)^{1/2}$; $\theta=\operatorname{arctg}(Y/X)$. Так так $\int\limits_{-\pi}^{\pi}p[\Phi\mid y(t)]\,d\Phi=1;\ K=[I_0(2RM)]^{-1}$, то $E[\Phi\mid y(t)]=\sum\limits_{n=1}^{\infty}\frac{2}{n}(-1)^{n+1}\sin n\theta\times$ $\times\frac{I_n(2RM)}{I_0(2RM)}$. Если $2RM\gg 1$, то приближенно эта оценка будет иметь вид $\sum\limits_{n=1}^{\infty}\frac{2}{n}(-1)^{n+1}\sin n\theta=\theta$, т. е. будет эквивалентна оценке максимального правдоподобия. (*Прим. авт.*).

Дисперсия ошибки, в общем, является довольно сложной функцией отношения сигнал/шум R. Однако если R велико, то величина θ_e с большой вероятностью будет малой. В результате выражение $(2R)^{1/2}\cos\theta_e$ будет велико и

$$\frac{1}{\sqrt{2\pi}}\int\limits_{-\infty}^{(2R)^{1/2}\cos\theta_e} e^{-x^2/2}\,dx \approx 1-\frac{\exp[-R\cos^2\theta_e]}{\sqrt{2\pi}\,(2R)^{1/2}\cos\theta_e}\,. \tag{3.66}$$

Следовательно,

$$p(\theta_e)\approx\left(\frac{R}{\pi}\right)^{1/2}\cos\theta_e\exp[-R\sin^2\theta_e]. \tag{3.67}$$

Более того, если θ_e мало, то $\cos\theta_e\approx 1$ и $\sin\theta_e\approx\theta_e$, так что

$$p(\theta_e)\approx\left(\frac{R}{\pi}\right)^{1/2}\exp[-R\theta_e^2]\,. \tag{3.68}$$

Ошибка θ_e имеет асимптотически гауссовское распределение с нулевым средним и дисперсией $\sigma^2{}_n=1/2R$. Снова, как легко проверить с помощью ф-лы (3.51), эта оценка асимптотически эффективна (при $\nu=1$); она не смещена и, когда R велико, имеет минимальную дисперсию, задаваемую ф-лой (2.66).

Если амплитуда сигнала распределена равномерно, то дисперсия сигнала имеет вид

$$\sigma_s^2=\frac{1}{2\pi}\int\limits_{-\pi}^{\pi}\Phi_\nu^2\,d\Phi_\nu=\frac{\pi^2}{3}\,. \tag{3.69}$$

Энергия принимаемого сигнала постоянна и равна $\mathscr{E}=A^2T_s$. Поэтому отношение сигнал/шум на выходе

$$\left(\frac{S}{N}\right)_{\text{ФТ}}\approx\frac{2\pi^2}{3}\,\frac{\mathscr{E}}{N_0}=\frac{\pi^2}{3}\left(\frac{S}{N}\right)_{\substack{\text{ког.}\\ \text{АИМ}}}\,. \tag{3.70}$$

Это приближенный результат, справедливый, когда отношение сигнал/шум на входе $\mathscr{E}/N_0$ достаточно велико.

Требования, предъявляемые к эффективной ширине полосы в случае ФТ, в точности такие же, как при некогерентной АИМ. Рассуждения, приведенные в § 3.6, непосредственно применимы и здесь. Следовательно, эффективная ширина полосы ФТ сигнала вдвое больше требуемой для когерентного АИМ сигнала, хотя на практике ширина полосы, которая должна быть отведена одному каналу в обоих случаях, по существу, одна и та же, что можно понять, рассматривая соответствующие этим сигналам спектры.

3.8. Заключительные замечания

В этой главе рассматривались наиболее важные свойства непрерывных по амплитуде импульсных систем связи, а именно: вид оптимальных демодуляторов (при различных определениях оптимальности); достижимое на выходе отношение сигнал/шум;

спектры сигнала и требования к эффективной ширине полосы. Были изучены три частные системы: когерентная АИМ, некогерентная АИМ и ФТ. При равномерном распределении выборок сигнала было найдено, что отношение сигнал/шум при ФТ больше, чем при когерентной АИМ в $\pi^2/3$ раз, а для некогерентной АИМ это отношение в четыре раза меньше, чем для когерентной АИМ. Спектры этих трех систем почти одинаковы, но эффективная ширина полосы равна $1/T_s$ герц для ФТ и некогерентной АИМ и $1/2T_s$ герц для когерентной АИМ.

Интересно отметить то количество априорной информации, которое должно быть использовано различными демодуляторами максимального правдоподобия. Для когерентного АИМ демодулятора [ср. с ф-лой (3.33)] предполагаются известными мощность принятого сигнала и фаза несущей сигнала, хотя от первого из этих требований часто можно отказаться, если важна только относительная амплитуда сигнала. При некогерентной АИМ демодуляции обходятся без знания фазы несущей, хотя правильно спроектированный демодулятор максимального правдоподобия требует знания как уровня мощности сигнала, так и уровня мощности шума [ф-ла(3.48)]. В случае ФТ нет необходимости знать амплитуду сигнала и уровень шума, но, очевидно, необходимо иметь в распоряжении опорную фазу, так как модулирующий сигнал может быть определен только лишь по разности между этой опорной фазой и фазой принятого сигнала. («Некогерентная» ФТ обсуждается в следующей главе.) Наконец, ФТ система обладает важным практическим преимуществом: постоянством передаваемой мощности. В противоположность этому при когерентной АИМ с равномерным распределением амплитуды сигнала требуется пиковая мощность, втрое большая ее средней мощности.

Хотя огибающие импульсов для каждой из рассмотренных в этой главе систем были прямоугольными, по существу, аналогичные результаты могли быть получены для произвольной формы огибающей $f(t)$. В частности, если фильтр приемника согласован с импульсом $f(t)\sin\omega_c t$; $0<t<T_s$, где $f(t)$ — медленно (по сравнению с периодом несущей $2\pi/\omega_c$) меняющаяся функция, и если принимаемый сигнал имеет вид $Af(t)\sin(\omega_c t+\Phi)+n(t)$, то отношение сигнал/шум на выходе фильтра равно

$$\frac{\left(A\int\limits_0^{T_s} f^2(t)\,dt\cos\Phi\right)^2}{\frac{N_0}{2}\int\limits_0^{T_s} f^2(t)\,dt} = 2\cos^2\Phi\,\frac{\mathcal{E}}{N_0}, \tag{3.71}$$

где $\mathcal{E}$ — энергия принятого сигнала, а N_0 — спектральная плотность шума. Очевидно, это отношение не зависит от формы огибающей импульса.

Более того, хотя оптимальные характеристики системы достигаются, когда фильтры приемника согласованы с принимаемым импульсом, однако метод исследования характеристик, изложенный в этой главе, в равной мере применим и тогда, когда, фильтры не являются согласованными. Если принимаемый импульс имеет вид, описанный в предыдущем абзаце, а импульсный отклик фильтра приемника — вид $h(t)\sin\omega_c(T_s-t)$, то отношение сигнал/шум на выходе

$$\frac{\left(A\int\limits_{-\infty}^{\infty} f(t)\,h(T_s-t)\,dt\cos\Phi\right)^2}{\frac{N_0}{2}\int\limits_{-\infty}^{\infty} h^2(T_s-t)\,dt} =$$

$$= 2\cos^2\Phi\,\frac{\mathcal{E}}{N_0}\,\frac{\left(\int\limits_{-\infty}^{\infty} f(t)\,h(T_s-t)\,dt\right)^2}{\int\limits_{-\infty}^{\infty} f^2(t)\,dt\int\limits_{-\infty}^{\infty} h^2(T_s-t)\,dt} \overset{\Delta}{=} 2\gamma\cos^2\Phi\,\frac{\mathcal{E}}{N_0}. \qquad (3.72)$$

Единственным результатом несогласованности фильтра будет снижение отношения сигнал/шум на выходе в γ раз [эта величина согласно неравенству Шварца меньше единицы, кроме случая, когда функция $h(T_s-t)$ отличается от $f(t)$ только множителем]. При этой модификации предыдущие методы могут быть использованы даже тогда, когда фильтры приемника несогласованные.

Это утверждение, очевидно, должно быть видоизменено, когда передается последовательность импульсов, а импульсный отклик $h(t)$ не равен тождественно нулю при $t>T_s$. В последнем случае на выход фильтра в моменты каждого отсчета влияют как более ранние импульсы, так и текущий импульс, и усредненная характеристика системы, в общем, хуже, чем предсказанная на основе рассмотрения одного единственного импульса. Более того, утверждение, что характеристика системы не зависит от формы импульса, также следует видоизменить, если канал связи не является каналом с бесконечной шириной полосы и белым гауссовским шумом, что здесь предполагалось. Если, например, ширина полосы канала невелика по сравнению с шириной полосы сигнала или если в канале имеется многолучевость с различными временами задержки в различных лучах, то характеристика системы в действительности будет функцией формы импульса.

Задачи

3.1. а) Показать, что если (гауссовский стационарный) шум не обязательно белый, то равенство (3.21) переходит в

$$p(\nu\,|\,y(t)) = Kp(\nu)\exp\left\{\int\limits_0^{T_s}[2Ay(t)\,z(t,\ \nu) - A^2x(t,\ \nu)\,z(t,\ \nu)]\,dt\right\},$$

где $z(t, \nu)$ определяется интегральным уравнением $x(t, \nu) = \int\limits_0^{T_s} R_n(t-\tau) z(\tau, \nu) d\tau$,

а $R_n(\tau)$ — автокорреляционная функция шума.

б) Пусть $y(t) = x(t, \nu) + n(t)$; $0 < t < T_s$, где $n(t)$ — гауссовский шум со спектральной плотностью мощности $S_n(\omega)$, и пусть $h(t)$ и $H(i\omega)$ — соответственно импульсный отклик и частотная характеристика *обеляющего фильтра,* определяемого равенством $|H(i\omega)|^2 S_n(\omega) = N_0/2$. Показать, что если $y(t)$ подается на вход такого фильтра, то выходом будет $y_f(t) = \xi(t, \nu) + n_w(t)$, где $\xi(t, \nu) = \int\limits_0^{T_s} x(\tau, \nu) h(t-\tau) d\tau$ и, где $n_w(t)$ — белый гауссовский процесс.

в) Показать, что приемник, полученный в п. а), может быть реализован как обеляющий фильтр, за которым следует приемник, который следовало бы использовать, если принимается сигнал из множества $\{\xi(t, \nu)\}$, определенного в п. б) на фоне белого гауссовского шума.

3.2. а) Найти спектр АИМ сигнала, определенного равенством (3.26), где ν_i — взаимонезависимые случайные величины, равномерно распределенные на интервале (a, b). Сравнить его со спектром сигнала $\sqrt{2} A m(t-\eta) \sin(\omega_c t + \Phi)$, где $m(t) = \nu_i$; $iT_s < t < (i+1) T_s$, а η и Φ — независимые случайные величины, равномерно распределенные на интервалах $(0, T_s)$ и $(0, 2\pi)$ соответственно.

б) Повторить п. а) для ФТ сигнала, определенного равенством (3.61), где величины Φ_i — равномерно распределены на интервале $(-\pi, \pi)$.

в) Повторить п. а) и б), когда огибающие импульсов *косинусоидальны,* а не прямоугольны, т. е. когда сигнал состоит из последовательности амплитудно- или фазовомодулированных импульсов вида $\sqrt{2} A p(t) \sin(\omega_c t + \Phi)$, где $p(t) = \sqrt{2/3}(1 - \cos 2\pi t/T_s)$.

3.3. Показать, что формула оценки, определяемая равенством (3.40), является оптимальной минимаксной формулой оценки амплитуды АИМ импульса при стоимостном критерии, определяемом среднеквадратической ошибкой, т. е. показать, что эта формула оценки минимизирует максимум возможной среднеквадратической ошибки, когда известна лишь дисперсия амплитуды сигнала (с нулевым средним). (*Указание.* Показать, что среди всех распределений с нулевым средним значением амплитуды и дисперсией σ^2_s гауссовское распределение приводит к наибольшей среднеквадратической ошибке, когда используется эта формула оценки.)

3.4. ФТ модулированный сигнал $s_i(t) = \sqrt{2} A \sin(\omega_c t + \Phi_i)$; $iT_s < t < (i+1) T_s$ принимается в присутствии белого гауссовского шума. Приемник строится так, чтобы получить оптимальную оценку $\hat{s}_i(t)$ принятого сигнала в смысле среднеквадратического критерия и использовать фазу этой оценки как оценку величины θ_i. Показать, что получающаяся в результате оценка совпадает с оценкой максимального правдоподобия величины θ_i.

Глава 4

ДИСКРЕТНЫЕ ПО АМПЛИТУДЕ И ПО ВРЕМЕНИ СИСТЕМЫ СВЯЗИ

4.1. Введение

Схемы импульсной модуляции, рассмотренные в предыдущей главе, были предназначены для сигналов, представлявших собой непрерывные функции некоторого параметра. Хотя оптимальный приемник для такого множества функций, очевидно, требует континуума согласованных фильтров, по одному на каждый возможный принятый сигнал, рассмотренные системы содержали лишь один или два таких фильтра.

Этот случай не является общим. (Рассмотрите, например, оптимальный демодулятор, когда множество сигналов имеет вид $s_\omega(t)=\sqrt{2}A\sin\omega t;\ 0<t<T_s$, где ω — непрерывный параметр.) В общем случае оптимальный приемник должен определять функцию принятого сигнала для каждого возможного значения оцениваемого параметра. В этих условиях для импульсной передачи непрерывного параметра могут быть построены лишь приближенно оптимальные приемники. Часто можно получить удобное приближение, если учесть, что выход фильтра, настроенного на сигнал $s_\alpha(t)$, будет, вообще говоря, большим, когда принимается сигнал $s_{\alpha'}(t)$ с параметром α', отличающимся лишь незначительно от параметра α. Можно предположить, что приемник будет «проквантован» плотным множеством согласованных фильтров, заменяющих теоретически необходимое бесконечное множество.

Хотя квантование сигнала на приемном конце упрощает систему связи, квантование на передающем конце приводит к еще большим упрощениям. Использование лишь конечного числа сигналов приводит, разумеется, к ошибкам квантования всякий раз, когда предназначенная для передачи информация по своей природе не является дискретной. Ошибка может быть, однако, абсолютно не существенной или даже полезной, так как почти при каждом мыслимом использовании этой информации требуется лишь определенная точность. И в любом случае (так как сигнал неизбежно искажается шумом) достижимая точность ограничена, независимо от используемого метода модуляции.

Можно утверждать, что потери при квантовании сигнала до его передачи малы и, кроме того, квантование приводит к ряду преимуществ. Основное преимущество квантования состоит в легкости накопления дискретной информации, а также ее перемещения или передачи из одного места в другое. Некоторые из менее очевидных преимуществ станут более ясными в последующих главах. Главное преимущество, которое использовано в этой главе, состоит в сравнительной простоте анализа и реализации таких систем.

Рассмотрим в общих чертах работу системы: на вход передатчика *дискретной системы связи* поступает последовательность цифр (в некоторой подходящей системе счисления). Он превращает эти цифры в последовательность *символов*, каждый из которых выбирается из конечного множества символов (будем называть его *алфавитом символов*) и однозначно соответствует некоторому заданному отрезку последовательности входных цифр. Каждый из этих символов представляется затем с помощью некоторого сигнала[1]) $s_\nu(t)$; $\nu=1, 2, \ldots, N$, где N обозначает число символов в алфавите. Каждые T_s секунд будет передаваться один символ; обычно предполагается, что сигнал $s_\nu(t)$ равен нулю вне интервала $(0, T_s)$.

Мерой качества систем связи, рассмотренных в предыдущей главе, было отношение сигнал/шум на выходе. Для дискретных систем также можно определить отношение сигнал/шум на выходе (принимая во внимание, если нужно, среднеквадратическую ошибку квантования). Однако более естественной и в большинстве случаев более удовлетворительной мерой качества является *вероятность ошибки в символе,* т. е. вероятность того, что символ на выходе приемника отличается от переданного. Критерий среднеквадратической ошибки в случае аналоговых систем полезен, главным образом, потому, что ее легко вычислить, а не потому, что она обязательно является мерой качества, наиболее интересной для потребителя. Фактически, как следует из замечаний, изложенных в предыдущих абзацах, постоянно существующие, но малые по сравнению с требуемой для принимаемой информации точностью ошибки передачи могут быть намного менее неприятными, чем редкие, но большие ошибки в этой информации. В то же время среднеквадратическая ошибка в этих случаях может быть одинаковой.

Вероятность ошибки в символе представляется разумной основой для сравнения двух систем, использующих одно и то же число символов. Но нужно сделать оговорку к этому утверждению, когда сравниваемые системы используют различное число символов. А именно, если алфавит сигналов содержит N символов, то каждый принятый символ переносит $\log_2 N$ бит информации (т. е. такое же количество информации, которое содержится в $\log_2 N$ двоичных символах). Ясно, что две системы, имеющие неравные числа символов, можно разумно сравнить только, если они используют одну и ту же энергию для передачи каждого бита информации. Стоимость передачи оценивается полной энергией, необходимой для передачи всего сообщения, а не энергией, необходимой для удовлетворительной передачи некоторого символа.

---

[1]) Обычно будем использовать слово «символ» как применительно к определенному выше символу, так и для сигнала, который его представляет. Аналогично термин «алфавит символов» будет обозначать как множество символов, так и множество соответствующих сигналов. *(Прим. авт.).*

Далее в этой главе мерой качества служит вероятность ошибки в символе. Чтобы сравнить системы, использующие различные числа символов, следует определить эту вероятность как функцию средней энергии, затрачиваемой на каждый бит переданной информации. В процессе вычисления вероятности ошибки в символе обычно одновременно определяются также вероятности ошибок каждого вида (вероятности ошибочно вынести решение в пользу $s_\nu(t)$ вместо $s_\mu(t)$ для любых μ и ν). Эти величины всегда по желанию можно использовать для вычисления среднеквадратической ошибки.

4.2. Оптимальный когерентный по фазе приемник и его характеристики

Если в гл. 3 рассматривалась статистическая оценка некоторого параметра принятого сигнала, то здесь задачей является проверка многих гипотез. Эта задача рассматривалась в § 2.8, где было отмечено, что оптимальное решение в случае, когда стоимость ошибки не зависит от конкретного вида ошибки, состоит в выборе гипотезы, имеющей наибольшую апостериорную вероятность быть верной. Так как требуется минимизировать вероятность ошибки, то при рассмотрении все ошибки равноценны, и оптимальный приемник фактически является *приемником максимальной апостериорной вероятности.*

Сигнал на входе приемника имеет вид $y(t)=As_{\nu_i}(t-iT_s)+n(t)$; $iT_s<t<(i+1)T_s$, для некоторого значения $\nu_i=1, 2, \ldots, N$[1]. Апостериорные вероятности $P[\nu|y(t)]$ легко определить в предположении, что шум — белый гауссовский. С помощью рассуждений, аналогичных проведенным в § 3.4, получаем

$$P[\nu|y(t)]=kP(\nu)\exp\left\{\frac{2A}{N_0}\int_0^{T_s} y(t)\,s_\nu(t)\,dt-\frac{A^2}{N_0}\int_0^{T_s} s_\nu^2(t)\,dt\right\}=$$

$$=k\exp\left\{\frac{2A}{N_0}\int_0^{T_s} y(t)\,s_\nu(t)\,dt-\frac{A^2K_\nu}{N_0}\right\}, \tag{4.1}$$

где k — постоянная, не зависящая от i, а постоянные

$$K_\nu=\int_0^{T_s} s_\nu^2(t)\,dt-\frac{N_0}{A^2}\log_e P(\nu) \tag{4.2}$$

не зависят от принятого сигнала $y(t)$. Оптимальное решение состоит в выборе сигнала $s_\mu(t)$, где μ — значение ν, которое максимизирует выражение

$$z_\nu=\int_0^{T_s} y(t)\,s_\nu(t)\,dt-\frac{AK_\nu}{2}\,. \tag{4.3}$$

---

[1] Как и в предыдущей главе, i полагается равным нулю, а подстрочный индекс у ν опускается, если это не будет вызывать недоразумений. (*Прим. авт.*).

Оптимальный приемник, таким образом, состоит из набора параллельно соединенных согласованных фильтров, как показано на рис. 4.1.

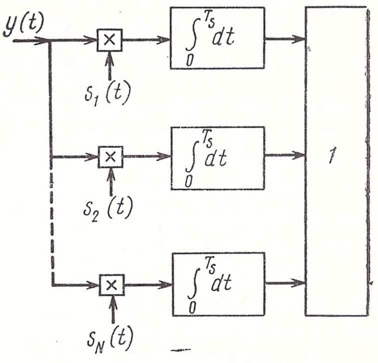


Рис. 4.1. Функциональная схема оптимального фазовокогерентного демодулятора (алфавит с N символами); 1 — устройство, выносящее решение; на выходе $\hat{s}(t)$

По предположению аддитивный шум $n(t)$ — белый и имеет гауссовское распределение. Тогда, если $y(t) = As_r(t) + n(t)$, то случайные величины z_i имеют гауссовское распределение для любого заданного значения r. Так как шум белый, то $E[n(t)] = 0$ и $E[n(u)n(t)] = (N_0/2)\,\delta(t-u)$, где N_0 — односторонняя спектральная плотность шума. Следовательно,

$$\eta_\nu(r) \underset{=}{\Delta} E(z_\nu \mid r) = A\int_0^{T_s} s_r(t)\, s_\nu(t)\, dt - \frac{AK_\nu}{2}, \tag{4.4}$$

а условная дисперсия случайной величины z_ν

$$\sigma_\nu^2(r) = \frac{N_0}{2}\int_0^{T_s} s_\nu^2(t)\, dt = \frac{N_0}{2A^2}\mathcal{E}_\nu = \sigma_\nu^2; \tag{4.5}$$

в ф-ле (4.5) $\mathcal{E}_\nu$ — энергия ν-го принятого символа. Условная ковариация величин z_ν и z_μ

$$\rho_{\nu\mu}(r) = \frac{E\{[z_\nu - \eta_\nu(r)]\,[z_\mu - \eta_\mu(r)] \mid r\}}{\sigma_\nu\ \sigma_\mu} =$$

$$= \frac{1}{\sigma_\nu\,\sigma_\mu}\frac{N_0}{2}\int_0^{T_s} s_\mu(t)\ s_\nu(t)\, dt \underset{=}{\Delta} \rho_{\nu\mu} = \boldsymbol{\rho}_{\mu\nu} \tag{4.6}$$

также не зависит от переданного символа.

Если передается сигнал $s_r(t)$, то вероятность правильного приема этого сигнала имеет вид

$$P_c(N;\, r) = \Pr[z_r > \max_{k \neq r} z_k \mid r] = \int_{-\infty}^{\infty}\int_{-\infty}^{w_r+\eta_r-\eta_1} \ldots \int_{-\infty}^{w_r+\eta_r-\eta_N} \times$$

$$\times \frac{\exp\left(-\frac{1}{2}\mathbf{w}^T \Lambda^{-1}\mathbf{w}\right)}{(2\pi)^{N/2}\,|\Lambda|^{1/2}}\, dw_1 \ldots dw_N\, dw_r, \tag{4.7}$$

где $w_i = z_i - \eta_i$; $\eta_i = \eta_i(r)$; $\mathbf{w}$ — вектор-столбец $(w_1, w_2, \ldots, w_N)$; $\mathbf{w}^T$ — транспонированный вектор-столбец, а Λ — (невырожденная) ковариационная матрица $\Lambda = \{\sigma_\nu \sigma_\mu \rho_{\mu\nu}\}$. Обозначение Λ^{-1} принято для матрицы, обратной Λ, а $|\Lambda|$ — ее определитель. Окончательно вероятность ошибки в рассматриваемой системе связи имеет вид

$$P_e(N) = 1 - \sum P(r) P_c(N;\ r), \tag{4.8}$$

где опять $P(r)$ — априорная вероятность символа $s_r(t)$. Вероятность ошибки, в принципе, может быть вычислена для любой невырожденной матрицы Λ по ф-ле (4.7). Но если на множество сигналов $\{s_i(t)\}$ наложены некоторые ограничения, то можно получить в некотором отношении более удобное для работы выражение. Как указывалось, оптимальный приемник принимает решения, используя величины, определенные равенством (4.3), и, следовательно, подразумевается, что известны амплитуда принятого сигнала A и спектральная плотность шума N_0. Если, однако, сделать K_ν независимым от ν, потребовав, чтобы энергия сигнала $\mathcal{E}_\nu$ и априорные вероятности $P(\nu)$ не зависели от ν, то ни один из этих параметров не нужно будет измерять при реализации оптимального приемника. Это требование удобно как с практической, так и с аналитической точки зрения.

Кроме того, передатчик может работать более эффективно, так как передаваемая энергия будет относительно постоянна. Поэтому указанные требования дают большие практические преимущества. Более того, они обычно не влияют на наиболее важные результаты. Средняя информация, передаваемая на один символ, очевидно, максимизируется, когда априорные вероятности символов равны. В гл. 10 рассматриваются методы, позволяющие приблизиться к этому случаю при произвольной статистике источника. А если каждый символ априори равновероятен, то каждый символ переносит одно и то же количество информации. Следовательно, на передачу каждого символа нужно тратить одну и ту же энергию, если этому не мешают другие обстоятельства.

Если источник осуществляет выбор из N символов, имеющих равные априорные вероятности, и всем символам соответствуют сигналы с равными энергиями, то оптимальный приемник просто вычисляет величины

$$z_\nu = \int_0^{T_s} y(t)\, s_\nu(t)\, dt \tag{4.9}$$

и выбирает наибольшую из них. В этом случае все еще применимо равенство (4.7) для вероятности правильного решения, но при этом $\eta_\nu(r) = A \int_0^{T_s} s_r(t) s_\nu(t) dt = A\,\mathcal{E}\rho_{\nu r}$ и

$$\sigma_\nu^2 = (N_0/2)\,\mathcal{E} = \sigma^2, \tag{4.10}$$

где $\rho_{ij} = \frac{1}{\mathcal{E}} \int_0^{T_s} s_i(t)\, s_j(t)\, dt$.

Равенство (4.7) лишь немного упрощается при этих предположениях относительно сигнала; вычисление вероятности ошибки все еще можно выполнить только с затратой значительных усилий. Поэтому рассмотрим несколько наиболее важных частных случаев.

Ортогональные символы. Если $\rho_{ij}=0$ для всех $i\neq j$, то множество символов по очевидным причинам называется ортогональным алфавитом. В этом случае равенство (4.7) можно значительно упростить. Прежде всего, в силу симметрии $P_c(N;\ r)$ не зависит от r. Вероятность правильного решения равна вероятности правильного определения (в приемнике) переданного сигнала независимо от того, какой частный сигнал был передан. Более того, так как $\rho_{ij}=0$, $i\neq j$, матрица $\mathbf{\Lambda}$ просто равна произведению σ^2 на единичную матрицу $\mathbf{I}$. Подставим эти соотношения в ф-лу (4.7)

$$P_e(N)=1-P_c(N)=1-\int\limits_{-\infty}^{\infty}\left[\int\limits_{-\infty}^{\zeta}\frac{e^{-\xi^2/2}}{\sqrt{2\pi}}\,d\,\xi\right]^{N-1}\frac{e^{-[\zeta-(2R)^{1/2}]/2}}{\sqrt{2\pi}}\,d\zeta\,\underline{\underline{\Delta}}\,\Phi_N\,(R_b), \tag{4.11}$$

где $R_b=R/\log_2 N=(\mathcal{E}/N_0)\log_2 N$ — отношение энергии принятого сигнала, приходящейся на один бит, к спектральной плотности шума. Следовательно, если $\rho_{ij}=0$ для всех $i\neq j$, то вероятность ошибки является функцией только числа сигналов N и отношения сигнал/шум на входе $R=\mathcal{E}/N_0$. Эта функция $\Phi_N(R_b)$ была найдена численно. Она изображена на рис. 4.2 как функция R_b для различных значений N.

Если имеются лишь два символа (двоичное ортогональное множество), то вероятность ошибки можно представить в несколько более удобной форме. Имеем

$$P_c(2)=\Pr\{z_1>z_2\mid 1\}=\Pr\{z_1-z_2>0\mid 1\}.$$

Так как z_1 и z_2 — независимые гауссовские случайные величины, то $z_1-z_2=w$ — также гауссовская величина со средним, равным разности средних величин z_1 и z_2, и дисперсией, равной сумме их дисперсий. Таким образом,

$$P_e(2)=\Pr\{w\leqslant 0\mid 1\}=\frac{1}{\sqrt{2\pi}}\int\limits_{R_b^{1/2}}^{\infty}e^{-\xi^2/2}\,d\,\xi\,\underline{\underline{\Delta}}\,\frac{1}{2}\left[1-\operatorname{erf}\left(\frac{R_b}{2}\right)^{1/2}\right]. \tag{4.12}$$

Вероятность ошибки, когда $\rho_{ij}=\rho$ для всех $i,\ j$, $i\neq j$. Если все коэффициенты взаимной корреляции $\rho_{ij}(i\neq j)$ равны ρ и каждый символ имеет одну и ту же энергию $\mathcal{E}$, то вероятность ошибки опять не зависит от переданного сигнала в силу имеющейся симметрии. Хотя можно ввести преобразование переменных в равенстве (4.7), которое сводит этот случай к только что рассмотренному ортогональному случаю, однако более простой метод определения вероятности ошибки состоит в следующем. Сначала предположим, что $\rho>0$, и рассмотрим множество сигналов, получаемое добавлением к каждому символу $s_j(t)$, $0<t<T'_s$, из ортогонального множества с N символами фиксированной функции

времени $r(t)$, $T'_s<t<T_s$. Корреляция между любыми из полученных символов имеет вид

$$\int_0^{T'_s} s_i(t)\,s_j(t)\,dt + \int_{T'_s}^{T_s} r^2(t)\,dt = \begin{cases} \mathcal{E}'', & i \neq j; \\ \mathcal{E}' + \mathcal{E}'' = \mathcal{E}, & i = j, \end{cases}$$

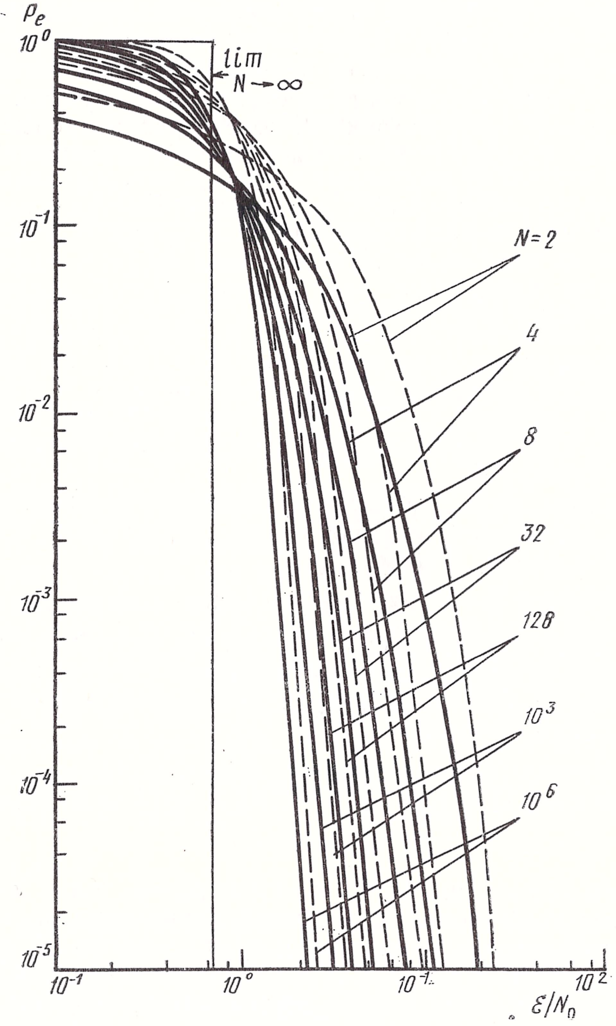


Рис. 4.2. Вероятности ошибок для ортогональных символов:
———— когерентная по фазе передача;
— — — — не когерентная по фазе передача

где $\mathcal{E}''$ — энергия $r(t)$; $\mathcal{E}'$ — энергия $s_i(t)$, а $\mathcal{E}$ — полная энергия каждого нового символа. Если $\mathcal{E}''/\mathcal{E} = \rho$, то множество новых символов, как и требовалось, содержит N символов, имеющих взаимокорреляционные коэффициенты $\rho_{ij}=\rho$, $i\neq j$. Но характеристики системы связи, использующей это множество сигналов, и системы с ортогональными символами эквивалентны. Последние $T_s-T'_s$ секунд при вычислении корреляции приводят к одинаковым результатам для всех N символов и, следовательно, не могут быть использованы при их различении. Использование определенных здесь новых символов, следовательно, эквивалентно использованию ортогонального множества символов, каждый из которых имеет энергию $\mathcal{E}'=\mathcal{E}-\mathcal{E}''=\mathcal{E}(1-\rho)$. Аналогично, если $\rho<0$, то можно начать с первоначального множества сигналов $\{s_i(t)\}$, $0<t<T_s$ и сформировать из него ортогональное множество, добавляя к каждому из символов функцию времени $r(t)$, $T_s<t<T'_s$, где $\int\limits_{T_s}^{T'_s} r^2(t)\,dt=|\rho|\,\mathcal{E}=-\rho\,\mathcal{E}$. Опять характеристики системы, использующей новые (ортогональные) символы, и системы, использующей первоначальные неортогональные символы, должны совпадать. Энергия новых символов равна $\mathcal{E}'=\mathcal{E}(1+|\rho|)=\mathcal{E}(1-\rho)$. Так как вероятность ошибки является функцией лишь коэффициентов ρ_{ij} и отношения сигнал/шум, то отсюда следует, что любое множество из N символов, каждый из которых имеет энергию $\mathcal{E}$, с коэффициентами взаимной корреляции $\rho_{ij}=\rho$ для всех i, j, $i\neq j$ приводит к той же самой вероятности ошибки, что и множество N ортогональных символов, имеющих энергию $\mathcal{E}(1-\rho)$; имеем

$$P_e(N,\ \rho)=\Phi_N\,[R_b(1-\rho)], \tag{4.13}$$

где Φ_N определяется так же, как в равенстве (4.11). Это справедливо как для положительных, так и для отрицательных ρ.

Об оптимальном выборе ρ. Как было показано выше, эффективная энергия некоторого множества сигналов равна $\mathcal{E}(1-\rho)$, где $\mathcal{E}$ — фактическая энергия каждого символа, а $\rho=\rho_{ij}$ — коэффициент взаимной корреляции. Казалось бы, что ρ следует сделать как можно бо́льшим и отрицательным ($\rho=-1$) для того, чтобы минимизировать вероятность ошибки. К сожалению, это возможно только тогда, когда $N=2$; в остальных случаях коэффициент ρ не может быть сделан столь малым. А именно, если алфавит состоит из N символов, то коэффициент ρ ограничен снизу величиной $-1/(N-1)$.

На самом деле можно доказать следующий более общий результат:

$$\rho_{\text{ср}} \triangleq \underset{\substack{i,j\\ i\neq j}}{\text{среднее}}\ \rho_{ij} = \frac{1}{N(N-1)}\sum_{\substack{i,\ j=1\\ i\neq j}}^{N}\rho_{ij}=\frac{1}{N(N-1)}\left\{\sum_{i,\ j=1}^{N}\rho_{ij}-N\right\}=$$

$$=\frac{1}{N(N-1)}\left\{\sum_{i,\ j=1}^{N}\frac{1}{\sigma_i\sigma_j}\,\frac{N_0}{2}\int\limits_{0}^{T_s}s_i(t)\,s_j(t)\,dt-N\right\}=$$

$$=\frac{1}{N(N-1)}\left\{\frac{N_0}{2}\int_0^{T_s}\left[\sum_{i=1}^{N}\frac{s_i(t)}{\sigma_i}\right]^2 dt-N\right\}\geqslant-\frac{1}{N-1}\,. \qquad (4.14)$$

Далее, так как $\rho_{\text{макс}} \triangleq \max\limits_{\substack{i,j\\ i\neq j}} \rho_{ij} \geqslant \rho_{\text{ср}}$, то и $\rho_{\text{макс}}$ и $\rho_{\text{ср}}$ не меньше $-1/(N-1)$. В частности, если $\rho_{ij}=\rho$ для всех i, j, $i\neq j$, то отсюда следует, что $\rho\geqslant -1/(N-1)$. Заметим также, что, если ρ равно $-1/(N-1)$, то множество сигналов *линейно зависимо,* т. е. $\sum\limits_{i=1}^{N} s_i(t)/\sigma_i=0$ для всех t, $0<t<T_s$.

Если N велико, то $\rho_{\text{макс}}$ и $\rho_{\text{ср}}$ ограничены снизу приближенно нулем, так что ортогональные алфавиты близки к оптимальному в смысле минимизации этих коэффициентов. Если $\rho_{ij}=-1/(N-1)$ для всех i, j, $i\neq j$, то вероятность ошибки такая же, как и для N-символьного ортогонального алфавита с энергией на символ, равной $[N/(N-1)]\mathcal{E}$. Такой алфавит называется *трансортогональным* алфавитом или *правильным симплексом.*

Можно было бы предположить, что так как эффективная энергия пропорциональна $1-\rho$, то оптимальные множества сигналов будут такими, для которых $\rho_{\text{макс}}$ (и $\rho_{\text{ср}}$) достигают минимального значения $-1/(N-1)$. Очевидно, это верно, когда все коэффициенты корреляции ρ_{ij} $(i\neq j)$ должны быть равными по условию. Но, хотя справедливость этого утверждения кажется интуитивно ясной даже для случая отсутствия условия равенства коэффициентов взаимной корреляции, оно остается гипотезой.

Биортогональные множества сигналов. Рассмотрим другой случай, представляющий определенный интерес. Пусть сигналы $s_1(t)$, $s_2(t)$, ..., $s_{N/2}(t)$ образуют множество $N/2$ ортогональных символов. Рассмотрим множество N символов $s_1(t)$, $s_2(t)$, ..., $s_{(N/2)+1}(t)=-s_1(t)$, $s_{(N/2)+2}(t)=-s_2(t)$, ..., $s_N(t)=-s_{N/2}(t)$. Тогда

$$\rho_{ij}=\begin{cases}0, & i\neq j, \quad j\pm N/2;\\ 1, & i=j;\\ -1, & i=j\pm N/2\end{cases}$$

и $$\rho_{\text{ср}}=\frac{1}{N(N-1)}\sum_{\substack{ij\\ i\neq j}}\rho_{ij}=-\frac{1}{N-1}\,.$$

Так как $\rho_{\text{макс}}=0>-1/(N-1)$, то это множество сигналов не оптимально в смысле, указанном выше, но $\rho_{\text{ср}}$ достигает нижней границы. Кроме того, как станет вскоре ясно, такое множество, называемое *биортогональным* алфавитом, имеет ряд значительных преимуществ перед ортогональным алфавитом. Так как обе функции, $s_i(t)$ и $-s_i(t)$, принадлежат алфавиту, то оптимальный приемник вычисляет величины $z_i=\int\limits_0^{T_s} y(t)s_i(t)dt$, $i=1, 2, \ldots, N/2$, где снова предполагается, что все сигналы имеют одинаковую энергию, появляются с равными априорными вероятностями. Приемником выбирается величина z_i, имеющая наибольшее абсолютное значение; знак z_i указывает, какой из сигналов $+s_i(t)$ или $-s_i(t)$ наиболее вероятен. Здесь, между прочим, проявляется одно из наиболее важных преимуществ использования биортогонального алфавита, а именно: необходимы лишь $N/2$ согласованных фильтров для приема N символов.

Вероятность правильного решения[1] $P_c(N)$ опять не зависит от того, какой из сигналов был передан, и равна вероятности того, что если был передан $s_{N/2}(t)$, то $z_{N/2} > |z_i|$ для всех $i < N/2$; имеем

$$P_c(N) = \Pr\left[z_{N/2} > \max_{i<N/2} |z_i| \;\middle|\; \frac{N}{2} \right].$$

Так как величина z_i имеет гауссовское распределение, причем

$$E(z_i \mid N/2) = \begin{cases} 0, & i < N/2; \\ A\mathscr{E}, & i = N/2 \end{cases} \quad \text{и} \quad \operatorname{var}(z_i \mid N/2) = \sigma_i^2 = (N_0/2A^2)\,\mathscr{E}, \text{ то}$$

$$P_e(N) = 1 - P_c(N) =$$

$$= 1 - \int_0^\infty \left[\int_{-\varsigma}^{\varsigma} \frac{e^{-\xi^2/2}}{\sqrt{2\pi}}\, d\xi \right]^{(N/2)-1} \frac{e^{-[\varsigma-(2R)^{1/2}]^2/2}}{\sqrt{2\pi}}\, d\zeta\ \Phi'_N(R_b), \tag{4.15}$$

где R_b определено ранее. Выражение (4.15) было найдено численными методами, а вероятности $\Phi'_N(R_b)$ изображены графически и табулированы, как функция R_b для различных значений N. При любом N имеем: $\Phi'_N(R_b) < \Phi_N(R_b)$, но различие становится незначительным для $N \geqslant 8$.

Вновь, если $N=2$, то вероятность ошибки может быть выражена с помощью интеграла вероятности в виде

$$P_e(2) = 1 - \frac{1}{\sqrt{2\pi}} \int_{-(2R_b)^{1/2}}^{\infty} e^{-\varsigma^2/2}\, d\zeta = \frac{1}{2}\left[1 - \operatorname{erf}\left(R_b^{1/2}\right)\right]. \tag{4.16}$$

Этот результат можно также получить, замечая, что ρ_{12} равно -1 для двухсимвольного биортогонального алфавита. Вероятность ошибки для биортогонального алфавита, когда $N=2$, равна вероятности ошибки для ортогонального алфавита с эффективным отношением сигнал/шум $R(1-\rho_{12}) = 2R$.

Границы вероятности ошибки. Выражение для вероятности ошибки в системе связи с N символами громоздко и с ним трудно работать, если нет никаких ограничений на коэффициенты корреляции ρ_{ij}, и даже в только что рассмотренных частных случаях вероятность можно найти лишь численно. К счастью, нетрудно получить простые границы для этого выражения, вполне удовлетворительные для многих конкретных приложений.

---

[1] Заметим, что ковариационная матрица Λ в этом случае вырождена так, что нельзя прямо применить равенство (4.7). *(Прим. авт.)*.

Простейшая и наиболее гибкая граница сверху для вероятности ошибки получается из *аддитивной границы,* использованной в § 2.8. Если выходы корреляторов приемника обозначить через z_i [ф-ла (4.9)][1]), то ошибка возникает, если был передан r-й символ, но $z_i \geqslant z_r$ для некоторого $i \neq r$. Так как эти события не являются взаимно исключающими, то

$$P_e(N;\ r) \leqslant \sum_{\substack{i=1\\ i\neq r}}^{N} \Pr\{z_i \geqslant z_r\} \leqslant (N-1) \max_{i\neq r} \Pr\{z_i \geqslant z_r\}. \tag{4.17}$$

Более того, так как вероятность, по крайней мере, одного из этих событий больше, чем вероятность какого-либо определенного из них, то

$$P_e(N;\ r) \geqslant \max_{\substack{i\\ i\neq r}} \Pr\{z_i \geqslant z_r\}. \tag{4.18}$$

Необходимо лишь повторить рассуждения, приводящие к ф-ле (4.12), чтобы получить

$$\frac{1}{2}\left\{1-\operatorname{erf}\left(\frac{R^*}{2}\right)^{1/2}\right\} \leqslant P_e(N;\ r) \leqslant \frac{(N-1)}{2}\left\{1-\operatorname{erf}\left(\frac{R^*}{2}\right)^{1/2}\right\}, \tag{4.19}$$

где $R^* = \min\limits_{i\neq r} R(1-\rho_{ir})$. Наконец, используя хорошо известные неравенства

$$\frac{e^{-x^2/2}}{\sqrt{2\pi}\,x}\left(1-\frac{1}{x^2}\right) \leqslant \frac{1}{2}\left[1-\operatorname{erf}\left(\frac{x}{\sqrt{2}}\right)\right] \leqslant \frac{e^{-x^2/2}}{\sqrt{2\pi}\,x},\quad x \geqslant 0,$$

находим, что

$$\frac{e^{-R^*/2}}{(2\pi R^*)^{1/2}}\left(1-\frac{1}{R^*}\right) \leqslant P_e(N;\ r) \leqslant \frac{1}{(2\pi R^*)^{1/2}} \exp\left\{-\frac{R^*}{2}+\log_e(N-1)\right\}. \tag{4.20}$$

Заметим, что верхняя граница для вероятности ошибки асимптотически стремится к нулю, когда $N\to\infty$, если $R^*/\log_2 N = R^*_b > 2\log_e 2$.

Более точная в общем случае граница сверху может быть получена с немного большими усилиями. Ограничим рассмотрение алфавитами с ортогональными символами, хотя результаты могут быть распространены также на произвольные множества сигналов. Из ф-лы (4.11) имеем

$$P_e(N) = \int\limits_{-\infty}^{\infty} \frac{e^{-(\zeta-\zeta_0)^2/2}}{\sqrt{2\pi}} \left\{1-\left[\frac{1}{2}\left(1+\operatorname{erf}\left(\frac{\zeta}{\sqrt{2}}\right)\right)\right]^{N-1}\right\} d\zeta, \tag{4.21}$$

---

[1]) Если априорные вероятности и энергии сигналов не одинаковы для всех символов, то z_i определяется равенством (4.3). *(Прим. авт.).*

где $\zeta^2{}_0=2R$. Но для $\zeta\geqslant 0$

$$\frac{1}{2}\left[1+\operatorname{erf}\left(\frac{\zeta}{2}\right)\right]=1-\int\limits_{\zeta}^{\infty}\frac{e^{-x^2/2}}{\sqrt{2\pi}}\,dx=1-\left[\int\limits_{\zeta}^{\infty}\int\limits_{\zeta}^{\infty}\frac{e^{-(x^2+y^2)/2}}{2\pi}\,dxdy\right]^{1/2}\geqslant$$

$$\geqslant 1-\left[\int\limits_{\sqrt{2}\,\zeta}^{\infty}\int\limits_{0}^{2\pi}\frac{e^{-r^2/2}}{2\pi}\,rd\theta\,dr\right]^{1/2}=1-\frac{1}{2}e^{-\zeta^2/2}\,. \tag{4.22}$$

Неравенство справедливо в силу того, что каждая из величин $x=r\sin\theta$ и $y=r\cos\theta$ больше, чем ζ, только если $0<\theta<\pi/2$ и $r\geqslant\sqrt{2}\,\zeta$; обратное неверно. Из (4.21) и (4.22), а также из замечаний, что $1+\operatorname{erf}(\zeta/\sqrt{2})\geqslant 0$ для всех ζ и что $(1-x)^{N-1}\leqslant 1-Nx$ для всех $x\geqslant 0$, получаем, что для любого $\zeta_1\geqslant 0$

$$P_e(N)\leqslant\int\limits_{-\infty}^{\zeta_1}\frac{e^{-(\zeta-\zeta_0)^2/2}}{\sqrt{2\pi}}\,d\zeta+\frac{N\,e^{-\zeta_0^2/4}}{2}\int\limits_{\zeta_1}^{\infty}\frac{e^{-(\zeta-\zeta_0/2)^2}}{\sqrt{2\pi}}\,d\zeta. \tag{4.23}$$

Эта верхняя граница минимизируется, если ζ_1 определяется равенством

$$\frac{N}{2}e^{-\zeta_1^2/2}=1, \tag{4.24}$$

так как тогда подынтегральное выражение первого члена меньше, чем подынтегральное выражение второго члена для всех $\zeta<\zeta_1$, и больше для всех $\zeta>\zeta_1$. Наконец, используя границу (4.22) и равенство (4.24), получим

$$P_e(N)\leqslant\int\limits_{\zeta_0-\zeta_1}^{\infty}\frac{e^{-\xi^2/2}}{\sqrt{2\pi}}\,d\xi+e^{-\frac{1}{2}\left(\frac{\zeta_0^2}{2}-\zeta_1^2\right)}\int\limits_{2\left(\zeta_1-\frac{\zeta_0}{2}\right)}^{\infty}\frac{e^{-\zeta^2/2}}{\sqrt{2\pi}}\,d\zeta\leqslant$$

$$\leqslant\begin{cases}\dfrac{1}{2}\left[e^{-\frac{(\zeta_0-\zeta_1)^2}{2}}+e^{-\left[\left(\zeta_1-\frac{\zeta_0}{2}\right)^2-\frac{1}{2}\left(\zeta_1^2-\frac{\zeta_0^2}{2}\right)\right]}\right]=e^{-\frac{(\zeta_0-\zeta_1)^2}{2}}, & \zeta_1<\zeta_0<2\zeta_1;\\[2ex] \dfrac{1}{2}e^{-\frac{(\zeta_0-\zeta_1)^2}{2}}+e^{-\frac{1}{2}\left(\frac{\zeta_0^2}{2}-\zeta_1^2\right)}\leqslant\dfrac{3}{2}e^{-\frac{1}{2}\left(\frac{\zeta_0^2}{2}-\zeta_1^2\right)}, & 2\zeta_1<\zeta_0,\end{cases} \tag{4.25}$$

где $\zeta^2{}_0=2R$ и $\zeta^2{}_1=2\log_e(N/2)$.

Вероятность ошибки стремится, следовательно, к нулю асимптотически по N, если $\zeta_0>\zeta_1$ и, следовательно, если $R_b>\log_e 2$. (Из рассмотрения аддитивной границы следует, что это заключение справедливо только, если $R_b>2\log_e 2$.) Нетрудно проверить, что это условие является необходимым и достаточным для того, чтобы вероятность ошибки асимптотически приближалась к нулю; так, в действительности $P_e(N)$ асимптотически равна единице, если $R_b<\log_e 2$.

4.3. Некогерентный по фазе прием

Для целей радиосвязи часто удобно представлять передаваемые символы в виде

$$s_i(t) = s_i(t, \Phi) = \sqrt{2}\,\xi_i(t)\sin(\omega_c t + \theta_j(t) + \Phi) =$$
$$= \sqrt{2}\,\alpha_i(t)\sin(\omega_c t + \Phi) + \sqrt{2}\,\beta_i(t)\cos(\omega_c t + \Phi), \quad 0 < t < T_s. \qquad (4.26)$$

Ранее, когда рассматривался случай точно известных ω_c и Φ такое представление не использовалось. Тогда не делалось никаких предположений относительно формы используемых символов, поскольку важны были только их коэффициенты корреляции. Если, однако, как в § 3.6, мы не хотим или не можем определить фазу несущей Φ, то принимаемый символ должен быть принят некогерентно и более детальное представление (4.26) необходимо для того, чтобы вычислить характеристики системы 1).

Если Φ, по предположению, является случайной величиной, равномерно распределенной на интервале $(0, 2\pi)$, а $\alpha_i(t)$ и $\beta_i(t)$ считаются известными функциями времени [предположения, которые состоятельны только, если $\alpha_i(t)$ и $\beta_i(t)$ медленно меняются по сравнению с $\sin(\omega_c t + \Phi)$], то легко определить оптимальный *фазовонекогерентный* приемник (см. § 3.6). Апостериорная вероятность того, что был передан i-й символ, если принят сигнал $y(t) = As_r(t, \Phi) + n(t)$, а фаза Φ известна, равна

$$P(i \mid y(t), \Phi) = K\exp\left[\frac{2A}{N_0}\int\limits_0^{T_s} y(t)\,s_i(t, \Phi)\,dt - \frac{\mathscr{E}_i}{N_0}\right]P(i \mid \Phi) =$$
$$= KP(i)\exp\left\{\frac{\mathscr{E}_i}{N_0} + \frac{2A}{N_0}\left[X_i\cos\Phi + Y_i\sin\Phi\right]\right\}, \qquad (4.27)$$

где K не зависит от i. Здесь $P(i)$ — априорная вероятность i-го символа и $\mathscr{E}_i = \int\limits_0^{T_s} A^2 s^2{}_i(t, \Phi)\,dt$; $X_i = \int\limits_0^{T_s} s_i(t, 0)\,y(t)\,dt$ и $Y_i = \int\limits_0^{T_s} s_i\left(t, \frac{\pi}{2}\right)y(t)\,dt$. Отсюда получаем, как в § 3,6, что

$$P(i \mid y(t)) = KP(i)\exp\left\{-\frac{\mathscr{E}_i}{N_0}\right\} I_0\left(\frac{2Az_i}{N_0}\right), \qquad (4.28)$$

где $z_i = (X^2{}_i + Y^2{}_i)^{1/2}$.

Если $P(i)$ и $\mathscr{E}_i$ не зависят от i, то (так как $I_0(x)$ — монотонно возрастающая функция x) $P(i \mid y(t))$ максимизируется, когда z_i

---

1) Сигнал, рассмотренный в § 3.6, имел вид (4.26) при $\beta_i(t) = 0$. Более общее выражение с необязательно равными нулю $\beta_i(t)$ позволяет рассматривать сигналы с угловой, а также амплитудной модуляцией. *(Прим. авт.)*.

достигает своего максимума. Следовательно, правило решения максимального правдоподобия (по максимуму апостериорной вероятности) утверждает, что μ-й символ принят тогда и только тогда, когда $z_\mu > \max\limits_{\nu\neq\mu} z_\nu$. Приемник, соответствующий этому правилу, изображен на рис. 4.3.

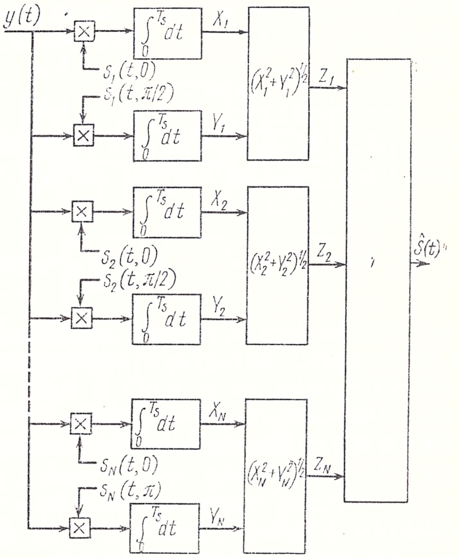


Рис. 4.3. Функциональная схема оптимального фазовонекогерентного демодулятора;
1 — устройство, выносящее решения

Другая интересная и полезная реализация оптимального некогерентного по фазе приемника получается при рассмотрении выхода фильтра, имеющего импульсный отклик

$$h_i(t) = \begin{cases} s_i(T_s - t, \Phi) & \text{при } 0 < t < T_s; \\ 0 & \text{в остальных случаях.} \end{cases} \qquad (4.29)$$

Если сигнал $y(t)$ подается на вход такого фильтра, то его выход в момент t имеет вид

$$\int_{-\infty}^{\infty} y(\tau) h_i(t-\tau)\, d\tau = \int_{t-T_s}^{t} y(\tau) s_i(T_s+\tau-t, \Phi)\, d\tau =$$

$$= Y_i(t)\cos(\omega_c t - \Phi') - X_i(t)\sin(\omega_c t - \Phi') = z_i(t)\cos[\omega_c t + \theta_i(t)], \qquad (4.30)$$

где

$$X_i(t) = \int_{t-T_s}^{t} y(\tau)\left[\sqrt{2}\,\alpha_i(T_s+\tau-t)\sin\omega_c\tau + \sqrt{2}\beta_i(T_s+\tau-t)\cos\omega_c\tau\right] d\tau;$$

$$Y_i(t) = \int_{t-T_s}^{t} y(\tau)\left[\sqrt{2}\,\alpha_i(T_s+\tau-t)\cos\omega_c\tau + \sqrt{2}\,\beta_i(T_s+\tau-t)\sin\omega_c\tau\right] d\tau;$$

$$\Phi' = \omega_c T_s + \Phi; \quad z_i(t) = (X_i^2(t) + Y_i^2(t))^{1/2};$$

$$\theta_i(t) = \operatorname{arctg}\left(\frac{Y_i(t)}{X_i(t)}\right) - \Phi'.$$

Выход этого фильтра является синусоидой с огибающей $z_i(t)$ и фазой $\theta_i(t)$. Так как $z_i(T_s)$ представляет собой решающую статистику z_i, определенную в ф-ле (4.28), то оптимальный приемник, очевидно, также можно реализовать с помощью параллельно соединенных фильтров, вид которых задается равенством (4.29), *детектора огибающей,* устройства, производящего выборки, и устройства, выносящего решение (рис. 4.4). Фильтр $h_i(t)$, который будем называть *некогерентным согласованным фильтром,* согласован с сигналом $s_i(t, \Phi)$ при произвольной фазе Φ. Интерпретация $z_i(t)$

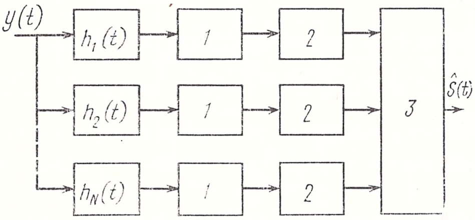


Рис. 4.4. Реализация схемы оптимального фазовонекогерентного демодулятора с помощью согласованных фильтров:

1 — детектор огибающей; *2* — устройство, производящее выборки; *3* — устройство, выносящее решения

как огибающей функции $z_i(t)\cos[\omega_c t+\theta_i(t)]$ является разумной, а реализация детектора огибающей для выделения этой огибающей возможна, если $z_i(t)$ и $\theta_i(t)$ относительно постоянны на любом $2\pi/\omega_c$-секундном интервале. Но так как изменения во времени $z_i(t)$ и $\theta_i(t)$ происходят всецело из-за изменений функций $\alpha_i(t)$ и $\beta_i(t)$, то фактически этот случай и имеет место.

В качестве первого шага при определении вероятностей правильного решения заметим, что X_i и Y_i являются гауссовскими случайными величинами, причем

$$\eta_x \overset{\Delta}{=} E\{X_i \mid r, \Phi\} = A\int_0^{T_s} s_r(t, \Phi)\, s_i(t, 0)\, dt = \frac{\mathcal{E}}{A}(\tilde{\rho}_{ir}\cos\Phi - \hat{\rho}_{ir}\sin\Phi); \quad (4.31)$$

$$\eta_y \overset{\Delta}{=} E\{Y_i \mid r, \Phi\} = \int_0^{T_s} s_r(t, \Phi) s_i\left(t, \frac{\pi}{2}\right) dt = \frac{\mathcal{E}}{A}(\hat{\rho}_{ir}\cos\Phi + \tilde{\rho}_{ir}\sin\Phi), \quad (4.32)$$

где

$$\tilde{\rho}_{ir} = \frac{1}{\mathcal{E}_0}\int_0^{T_s} [\alpha_i(t)\,\alpha_r(t) + \beta_i(t)\,\beta_r(t)]\, dt;$$

$$\hat{\rho}_{ir} = \frac{1}{\mathcal{E}_0}\int_0^{T_s} [\alpha_i(t)\,\beta_r(t) - \beta_i(t)\,\alpha_r(t)]\, dt \quad (4.33)$$

и $\mathcal{E} = \mathcal{E}_i$ — энергия принятого сигнала, по предположению независящая от i, а $\mathcal{E}_0 = \mathcal{E}/A^2$. Частота несущей ω_c по сравнению с максимальной существенной частотой модуляции предполагается достаточно высокой для того, чтобы можно было пренебречь интегралами от компонент удвоенной частоты. Это предположение используется и в дальнейшем. Кроме того, так как $\tilde{\rho}_{ii} = 1$ и $\hat{\rho}_{ii} = 0$, то находим, что

$$\operatorname{var}\{X_i \mid r, \Phi\} = \mathcal{E}_0 \frac{N_0}{2} = \operatorname{var}\{Y_i \mid r, \Phi\} \overset{\Delta}{=} \sigma^2; \quad (4.34)$$

$$E\{X_i Y_i \mid r, \Phi\} - E\{X_i \mid r, \Phi\}\, E\{Y_i \mid r, \Phi\} = 0.$$

Следовательно.

$$p(X_i,\ Y_i \mid r,\ \Phi) = \frac{\exp\left[-\dfrac{(X_i-\eta_x)^2}{2\sigma^2}\right]}{\sqrt{2\pi}\,\sigma}\ \frac{\exp\left[-\dfrac{(Y_i-\eta_y)^2}{2\sigma^2}\right]}{\sqrt{2\pi}\,\sigma}\,. \tag{4.35}$$

Положив $z_i=(X^2{}_i+Y^2{}_i)^{1/2}$, $\theta_i=\mathrm{arctg}\,(Y_i/X_i)$, $a_i=\tilde{\rho}_{ir}\mathscr{E}_0$ и $b_i=\hat{\rho}_{ir}\mathscr{E}_0$ и предполагая, что $p(\Phi|r)=p(\Phi)=1/2\pi$, $0\leqslant\Phi<2\pi$, получаем, что для $z_i\geqslant 0$

$$p(z_i \mid r) = \int\limits_{-\infty}^{\infty}\int\limits_{-\infty}^{\infty} p(z_i,\ \theta_i \mid r,\ \Phi)\,p(\Phi)\,d\Phi\,d\theta_i =$$

$$= \frac{z_i}{\sigma^2}\exp\left[-\frac{z_i^2+a_i^2+b_i^2}{2\sigma^2}\right] I_0\left(\frac{(a_i^2+b_i^2)^{1/2}z_i}{\sigma^2}\right). \tag{4.36}$$

Эта функция иногда называется райсовской плотностью распределения. Если $a_i=b_i=0$, то функция $p(z_i|r)$ сводится к релеевской плотности распределения:

$$p(z_i \mid r) = \frac{z_i}{\sigma^2}\exp\left(-\frac{z_i^2}{2\sigma^2}\right),\quad z_i\geqslant 0; \tag{4.37}$$

$$p(y_i=z_i^2 \mid r) = \frac{1}{2\sigma^2}\exp\left[-\frac{y_i}{2\sigma^2}\right],\quad y_i\geqslant 0, \tag{4.38}$$

где $p(y_i)$ — плотность известного χ-квадрат распределения с двумя степенями свободы.

Вероятность правильного решения $P_c(N)$, очевидно, выражается через совместную плотность распределения $p(z_1, z_2, \ldots, z_N|r)$, а не только через одномерные плотности распределения; имеем

$$P_c(N) = \sum P(r)\,P_c(N;\ r), \tag{4.39}$$

где $P_c(N;\ r)=\Pr\{z_r>\max\limits_{k\neq r} z_k|r\}$ [ср. с равенствами (4.7) и (4.8)]. Не удивительно, что с этим выражением иметь дело даже труднее, чем с соответствующим выражением в случае когерентного приема. Как и ранее, нужно наложить некоторые ограничения на величины $\tilde{\rho}_{ij}$ (и $\hat{\rho}_{ij}$), чтобы получить выражение, с которым легче работать.

Ортогональные символы. Если $\tilde{\rho}_{ij}=\hat{\rho}_{ij}=0$ для всех $i,\ j,\ i\neq j$, то говорят, что символы ортогональны. Вероятность ошибки в этом случае определяется довольно легко. Так как все гауссовские случайные величины X_i и Y_i взаимно не коррелированы и, следовательно, статистически независимы [т. е. так как $E(X_iX_j)-$ $-E(X_i)E(X_j)=E(Y_iY_j)-E(Y_i)E(Y_j)=\dfrac{N_0\mathscr{E}_0}{2}\tilde{\rho}_{ij}$ и $E(X_iY_j)-$ $-E(X_i)E(Y_j)=\dfrac{N_0\mathscr{E}_0}{2}\hat{\rho}_{ij}$ для всех $i,\ j$], то случайные величины z_i как функции независимых случайных величин также независимы.

Более того, в силу симметрии вероятность ошибки опять не зависит от передаваемого сигнала. В результате имеем

$$P_c(N) = \Pr\{z_1 > \max_{k \neq 1} z_k \mid r = 1\} = \int_{-\infty}^{\infty} p(z_1 \mid 1) \left[\int_{-\infty}^{z_1} p(z_i \mid 1)\, dz_i \right]^{N-1} dz_1. \tag{4.40}$$

Из ф-л (4.37) и (4.38) имеем

$$\int_{-\infty}^{z_1} p(z_i \mid 1)\, dz_i = \frac{1}{2\sigma^2} \int_0^{z_1^2} e^{-y/2\sigma^2}\, dy = 1 - e^{-\frac{z_1^2}{2\sigma^2}}, \quad i \neq 1 \tag{4.41}$$

и, используя это равенство с равенствами (4.36) и (4.40) и полагая $\zeta = z/\sigma$ и $\zeta_0 = (2R)^{1/2} = (2\mathcal{E}/N_0)^{1/2}$, получаем

$$P_c(N) = \int_0^{\infty} \zeta \exp\left[-\frac{\zeta^2 + \zeta_0^2}{2} \right] I_0(\zeta\zeta_0) \left(1 - e^{-\frac{\zeta^2}{2}} \right)^{N-1} d\zeta. \tag{4.42}$$

Используя биномиальное разложение

$$(1 - e^{-\zeta^2/2})^{N-1} = \sum_{i=0}^{N-1} \binom{N-1}{i} (-1)^i e^{-i\zeta^2/2},$$

находим, что

$$P_c(N) = e^{-\frac{\zeta_0^2}{2}} \sum_{i=0}^{N-1} \binom{N-1}{i} (-1)^i \int_0^{\infty} \zeta\, e^{-\frac{\zeta^2(i+1)}{2}} I_0(\zeta\zeta_0)\, d\zeta. \tag{4.43}$$

Последний интеграл можно вычислить:

$$\int_0^{\infty} \zeta\, e^{-\frac{\zeta^2(i+1)}{2}} I_0(\zeta\zeta_0)\, d\zeta = \frac{1}{i+1} \exp\left\{ \frac{\zeta_0^2}{2(i+1)} \right\}, \tag{4.44}$$

так что

$$P_c(N) = e^{-R} \sum_{j=1}^{N} \binom{N}{j} (-1)^{j-1} e^{R/j} = 1 - \frac{1}{N} \sum_{j=2}^{N} \binom{N}{j} (-1)^j e^{-\frac{j-1}{j}R}; \tag{4.45}$$

здесь использовано тождество $\binom{N-1}{i} \frac{1}{i+1} = \binom{N}{i+1} \frac{1}{N}$ и положено $j = i + 1$.

Вероятность ошибки при некогерентном приеме $P_e(N) = 1 - P_c(N)$ также была найдена численно. Она изображена на рис. 4.2 как функция $R_b = R/\log_2 N$ для различных значений N. Заметим, что если $N = 2$, то

$$P_e(2) = 1 - P_c(2) = \frac{1}{2} e^{-R/2}. \tag{4.46}$$

Неортогональные символы. Выражения для вероятностей ошибок при некогерентном по фазе приеме неортогональных символов обычно получить труднее, чем соответствующие результаты для когерентного по фазе приема. Приведенные выше рассуждения, например, относительно метода рассмотрения множества символов, имеющих одинаковые коэффициенты взаимной корреляции $\rho_{ij}=\rho$, как состоящего частично из ортогональных и частично из совпадающих отрезков функций, имеют небольшую ценность в некогерентном случае, так как совпадающие функции влияют на решение. Пусть $X_i=x_i+\alpha$ и $Y_i=y_i+\beta$, $i=1, 2, \ldots, N$, где α и β не зависят от i, а x_i, x_j, y_i и y_j взаимно независимы при всех i и j, $i\neq j$. Оптимальное решение строится на основе максимизации выражения $z_i=(X^2_i+Y^2_i)^{1/2}=(x^2_i+y^2_i+2\alpha x_i+2\beta y_i+\alpha^2+\beta^2)^{1/2}$. Наличие перекрестных членов αx_i и βy_i не дает возможности сказать, что решение не зависит от α и β, даже если эти члены являются общими для всех X_i и Y_i соответственно.

Тем не менее можно получить компактное выражение для вероятности правильного решения $P_c(N, \rho)$ при некогерентном приеме символов, имеющих одинаковые коэффициенты взаимной корреляции $\tilde{\rho}_{ij}=\rho\geqslant 0$, если $\hat{\rho}_{ij}=0$. А именно,

$$P_c(N, \rho)=(1-\rho)e^{-R}\int\limits_0^\infty\int\limits_0^\infty xy\exp\left[-\frac{1}{2}(x^2+y^2)\right] I_0\left[2R(1-\rho)^{1/2}x\right]\times$$

$$\times I_0(\rho xy)\left[1-Q\left(\sqrt{\rho}\,y, x\right)\right]^{N-1}dx\,dy, \tag{4.47}$$

где $Q(\alpha, \beta)=\int\limits_\beta^\infty x\exp\left(-\frac{1}{2}(x^2+\alpha^2)\right)I_0(\alpha x)dx$ — табулированная функция, известная под названием Q-функции Маркума. Вывод этой формулы довольно длинен и не будет здесь воспроизведен. Вероятность ошибки $P_e(N, \rho)=1-P_c(N, \rho)$ была найдена численно и табулирована.

Если $N=2$, то вероятность ошибки при некогерентном по фазе приеме является функцией лишь R и $\rho \triangleq (\tilde{\rho}^2_{12}+\hat{\rho}^2_{12})^{1/2}$. Найдено полезное выражение для этой вероятности, а именно,

$$P_e(2, \rho)=\frac{1}{2}e^{-\frac{R}{2}}\left[I_0\left(\frac{\rho R}{2}\right)+2\sum_{n=1}^{\infty}\left(\frac{1-\sqrt{1-\rho^2}}{\rho}\right)^n I_n\left(\frac{\rho R}{2}\right)\right]. \tag{4.48}$$

Границы для вероятности ошибки. Неравенства (4.20), конечно, в равной мере применимы и для некогерентного по фазе приема и показывают, что для произвольных значений $\rho_{ij}=(\tilde{\rho}^2_{ij}+\hat{\rho}^2_{ij})^{1/2}$

$$\max_{i\neq r} P_e\{2, \rho_{ir}\}\leqslant P_e(N; r)\leqslant\max_{i\neq r}(N-1)P_e\{2, \rho_{ir}\}. \tag{4.49}$$

Вероятность $P_e\{2, \rho_{ir}\}$, определенная ф-лой (4.48), легко оценить. Так как

$$0 \leqslant I_n(x) = \frac{1}{\pi}\int\limits_0^{\pi} e^{x\cos\theta}\cos n\theta\, d\theta \leqslant \frac{1}{\pi}\int\limits_0^{\pi} e^{x\cos\theta}\, d\theta = I_0(x) \tag{4.50}$$

и

$$1 \leqslant I_0(x) \leqslant \frac{1}{\pi}\int\limits_0^{\pi} e^{x}\, d\theta = e^{x}, \tag{4.51}$$

то из ф-лы (4.48) следует, что

$$\frac{1}{2}e^{-\frac{R}{2}} \leqslant P_e(2, \rho) \leqslant \frac{1}{2}e^{-\frac{R}{2}} I_0\left(\frac{\rho R}{2}\right)\times$$

$$\times\left[1 + 2\sum_{n=1}^{\infty}\left(\frac{1-\sqrt{1-\rho^2}}{\rho}\right)^n\right] \leqslant \frac{1}{2}\left(\frac{1+\rho}{1-\rho}\right)^{1/2} e^{-\frac{R(1-\rho)}{2}}. \tag{4.52}$$

Так как граница сверху для $P_e(2, \rho)$ — монотонно возрастающая функция ρ, то $P_e(N;\, r)$ можно оценить с помощью величины $\rho_r \triangleq \max\limits_{i\neq r}(\tilde{\rho}^2_{ir}+\hat{\rho}^2_{ir})^{1/2}$. Фактически, кажется очевидным, что вероятность ошибки $P_e(N;\, r)$ достигает своего минимума, когда $\rho_r=0$. Так как решение основывается на абсолютных значениях решающих переменных, то отрицательные значения $\tilde{\rho}_{ij}$ и $\hat{\rho}_{ij}$, по-видимому, будут также неприятны, как и положительные значения. По крайней мере, интуитивно кажется, что оптимальным множеством символов для случая некогерентного по фазе приема будет ортогональное множество.

Интересно сравнить эту границу сверху для вероятности ошибки в случае некогерентного приема с соответствующей границей для вероятности ошибки в случае когерентного приема [см. (4.20)]. Из ф-л (4.49) и (4.52) для некогерентного приема имеем

$$P_e(N;\, r) \leqslant \frac{1}{2}\left(\frac{1+\rho_r}{1-\rho_r}\right)^{1/2}\exp\left\{-\frac{R}{2}(1-\rho_r) + \log_e(N-1)\right\}. \tag{4.53}$$

Аналогичный результат для когерентного приема равен границе (4.53), умноженной на $(2/(1+\rho_r)\pi R)^{1/2}$. Величины ρ_r не обязательно, однако, одинаковы в обоих случаях.

Рассуждения, которые приводят к границе (4.25) для вероятности ошибки при когерентном приеме ортогональных символов, применимы также и здесь после небольшой модификации. Используя ф-лы (4.42) и выражения для границы сверху (4.50) и (4.51) для $I_0(x)$, получаем, что при $\zeta^2{}_0=2R$

$$P_e(N) \leqslant \int\limits_0^{\infty}\zeta e^{-\frac{(\zeta-\zeta_0)^2}{2}}\left[1-(1-e^{-\zeta^2/2})^{N-1}\right]d\zeta =$$

$$= \int\limits_0^{\zeta_1} e^{-(\zeta-\zeta_0)^2}\, d\zeta + N e^{-\frac{\zeta_0^2}{4}}\int\limits_{\zeta_1}^{\infty}\zeta e^{-\left(\frac{(\zeta-\zeta_0)^2}{4}\right)}\, d\zeta \tag{4.54}$$

для любых $\zeta_1 \geqslant 0$. Определяя $e^{\zeta_1^2/2} = N/2$ и считая, что $P_0(N)$ представляет верхнюю границу в ф-ле (4.25) для вероятности ошибки в случае когерентного приема, для всех $\zeta_0 > \zeta_1$ имеем

$$P_e(N) - \sqrt{2\pi}\,\zeta_0 P_0(N) \leqslant \int\limits_0^{\zeta_1} (\zeta - \zeta_0)\, e^{-\frac{(\zeta-\zeta_0)^2}{2}}\, d\zeta +$$

$$+ 2e^{\frac{1}{2}\left(\zeta_1^2 - \frac{\zeta_0^2}{2}\right)} \int\limits_{\zeta_1}^{\infty} \left(\zeta - \frac{\zeta_0}{2}\right) e^{-\left(\zeta - \frac{\zeta_0}{2}\right)^2} d\zeta \leqslant e^{-(\zeta_0-\zeta_1)^2/2} \leqslant P_0(N), \qquad (4.55)$$

так что $P_e(N) \leqslant \left(2\sqrt{\pi R} + 1\right) P_0(N)$.

Границы вероятности ошибки при некогерентном приеме являются, очевидно, экспоненциально совпадающими со сравнимыми с ними границами для случая когерентного приема, и условие, накладываемое на R_b для того, чтобы соответствующие границы для ошибок были малыми, когда N велико, является одним и тем же в обоих случаях. Это не удивительно, так как фаза несущей, по предположению, остается постоянной во всем интервале некогерентного приема. При $N \to \infty$ интервал, на котором производится прием, также стремится к бесконечности и фаза сигнала, фактически, оценивается безошибочно.

4.4. Генерирование ортогональных символов

В нескольких предыдущих параграфах рассматривались характеристики систем связи, использующих конечные множества символов. Как было показано, вероятность ошибочного решения на приемном конце является функцией лишь числа символов N, их коэффициентов взаимной корреляции ρ_{ij} и отношения R_b энергии символа на бит к спектральной плотности шума. Утверждалось также, что оптимальные значения коэффициентов взаимной корреляции при отсутствии каких-либо других ограничений равны $\rho_{ij} = -1/(N-1)$ для когерентных по фазе систем и $\rho_{ij} = 0$ для некогерентных по фазе систем при всех $i, j, i \neq j$. Следовательно, когда N велико, ортогональное множество символов, по существу, является оптимальным для обеих ситуаций. Очевидно, важно уметь конструировать такое множество символов, которое можно использовать в практических системах. В этом параграфе описаны два легко реализуемых и широко используемых ортогональных множества символов и исследованы их эффективные полосы.

Символы для частотной манипуляции. Множество символов, используемых в системе связи с (дискретной) *частотной манипуляцией* (ЧТ)[1], имеет вид

$$s_i(t) = \sqrt{2} \sin\left(\omega_c + \frac{\pi k_i}{T_s}\right) t, \quad i = 0, 1, 2, \ldots, N-1, \qquad (4.56)$$

---

[1] ЧТ — частотная телеграфия. (*Прим. отв. ред.*)

где $\omega_c=\pi l/T_s$, а l и постоянные k_i — целые числа. Коэффициенты взаимной корреляции

$$\rho_{ij}=\frac{2}{T_s}\int_0^{T_s}\sin\left(\omega_c+\frac{\pi k_i}{T_s}\right)t\sin\left(\omega_c+\frac{\pi k_j}{T_s}\right)tdt=\begin{cases}1, & k_i=k_j;\\ 0 & k_i\neq k_j,\end{cases} \tag{4.57}$$

и сигналы $s_i(t)$ ортогональны независимо от величины N. Ортогональность в фазовонекогерентном смысле накладывает, однако, дополнительные ограничения на целые числа k_i. Положив

$$s_i(t,\Phi)=\sqrt{2}\sin\left(\omega_ct+\frac{\pi k_i}{T_s}t+\Phi\right)=\sqrt{2}\cos\frac{\pi k_i}{T_s}t\sin(\omega_ct+\Phi)+$$
$$+\sqrt{2}\sin\frac{\pi k_i}{T_s}t\cos(\omega_ct+\Phi)=\sqrt{2}\,\alpha_i(t)\sin(\omega_ct+\Phi)+\sqrt{2}\beta_i(t)\cos(\omega_ct+\Phi), \tag{4.58}$$

находим, что

$$\hat{\rho}_{ij}=\frac{1}{T_s}\int_0^{T_s}[\alpha_i(t)\beta_j(t)-\beta_i(t)\alpha_j(t)]\,dt=0, \tag{4.59}$$

только если k_i-k_j — четное целое число.

Множество ортогональных символов, удовлетворительное для когерентного и некогерентного по фазе приемов, определяется тогда равенством (4.56). Так как частоты сигналов должны быть разделены хотя бы интервалом $1/2T_s$ герц, чтобы гарантировать ортогональность в случае когерентности по фазе, то *эффективная ширина полосы* такого множества в соответствии с определением § 3.3 равна $N/2T_s$, где N обозначает общее число символов. Если ортогональные символы используются в некогерентной по фазе системе, то эффективная ширина полосы вдвое больше этой величины.

Биортогональное множество всегда можно получить из ортогонального (когерентного по фазе) множества просто добавлением символов $-s_i(t)$, $i=1, 2, \ldots, N$ к первоначальному множеству. Эта процедура не увеличивает ширину полосы по сравнению с ортогональным множеством, однако она удваивает число символов. Следовательно, эффективная ширина полосы биортогонального множества равна $N/4T_s$, что составляет половину полосы ортогонального множества того же самого объема.

Спектр мощности случайной последовательности каких-либо из этих символов может быть найден с помощью метода § 3.3.

Время-импульсная манипуляция. Вторым множеством сигналов, с которым часто приходится встречаться, является следующее:

$$s_i(t)=\begin{cases}\sqrt{2N}\sin\omega_ct & \text{при } \frac{iT_s}{N}<t<(i+1)\frac{T_s}{N};\\ 0 & \text{в остальных случаях.}\end{cases} \tag{4.60}$$

Обычно, чтобы сохранить одну и ту же энергию импульса, выбирают $\omega_c = l\pi N/T_s$, где l — целое или $l \gg 1$. Символы представляются с помощью импульсов, положение которых и определяет соответствующий символ. Система связи, использующая эти символы, называется системой с *время-импульсной манипуляцией* (ВИМ). Так как импульсы могут появляться только в моменты $t = iT_s/N$, рассматриваемая здесь система является дискретной ВИМ.

Определенные равенством (4.60) импульсы не перекрываются во времени; они, очевидно, ортогональны в обоих — фазово-когерентном и фазово-некогерентном — смыслах. Эффективная ширина полосы равна $N/2T_s$ герц в случае приема, когерентного по фазе. Имеем

$$2N \int\limits_{iT_s/N}^{(i+1)T_s/N} \sin\omega_{c_1} t \sin\omega_{c_2} t\, dt = 0,$$

если ω_{c1} и ω_{c2} отличаются на целое, кратное величине $\pi N/T$ рад/с. В результате не возникнет интерференция между любыми двумя одинаковыми ВИМ каналами до тех пор, пока их несущие частоты будут отличаться на целое, кратное величине $N/2T_s$ герц.

То же самое множество символов в случае некогерентного приема требует вдвое большей эффективной ширины полосы. Это происходит потому, что перекрестный член $2N \int\limits_{iT_s/N}^{(i+1)T_s/N} \sin\omega_{c1} t \cos\omega_{c2} t\, dt$ обращается в нуль, если потребовать, чтобы разность $\omega_{c1} - \omega_{c2}$ равнялась целому, кратному величине $2\pi N/T_s$.

Опять с помощью добавления отрицательных импульсов $-s_i(t)$, $i = 1, 2, \ldots, N$ число символов можно удвоить. В результате получим фазовокогерентное биортогональное множество, эффективная ширина полосы которого равна половине полосы ортогонального множества, содержащего то же самое число символов.

Существуют, конечно, многие другие используемые на практике методы генерирования ортогональных множеств сигналов. Один из методов, имеющий особое значение, подробно рассмотрен в гл. 13.

4.5. Фазовая манипуляция (ФТ). Когерентный по фазе прием

Еще одним множеством сигналов, представляющим некоторый интерес, является следующее:

$$s_i(t) = \sqrt{2}\sin(\omega_c t + \Phi_i), \quad 0 < t < T_s, \tag{4.61}$$

где $\Phi_i = 2\pi i/N$, $i = 0, 1, 2, \ldots, N-1$ и $\omega_c = \pi l/T_s$ для некоторого целого l. Система, использующая это множество символов, отличается от рассмотренной в гл. 3 ФТ системы только тем, что здесь число фаз сигнала конечно. Термин ФТ будет применяться к обеим этим системам с оговоркой в тех случаях, когда имеется опасность недоразумения.

Коэффициенты взаимной корреляции при ФТ (случай когерентной фазы)

$$\rho_{ij}=\cos(i-j)\frac{2\pi}{N}\,. \tag{4.62}$$

Если N равно 2, то ρ_{ij} равно -1 для $i\neq j$, и множество является оптимальным в смысле § 4.2. Если N равно 3, то ρ_{ij} равно $-1/2$, $i\neq j$ и снова множество оптимально. Если N равно 4, то ρ_{ij} равно 0 для $|i-j|=1$ или 3 и ρ_{ij} равно -1 для $|i-j|=2$. Это множество является биортогональным и, как таковое, минимизирует усредненный коэффициент взаимной корреляции. Вероятности ошибок в этих случаях уже были определены в § 4.2. Для больших значений N, однако, точные выражения для вероятностей ошибок, полученные в § 4.2, перестают быть применимыми, так как ρ_{ij} не являются независимыми от i и j для $i\neq j$ и множество не является биортогональным. Выражения для границ, приведенные в § 4.2, конечно, остаются применимыми. Однако в случае ФТ границы можно существенно уточнить.

Легко найти для ФТ приемник максимальной апостериорной вероятности. Согласно равенству (3.62)

$$P[\Phi_i\mid y(t)]=KP(\Phi_i)\exp\left\{\frac{2A}{N_0}\int_0^{T_s}y(t)\sqrt{2}\sin\omega_c t\,dt\cos\Phi_i+\right.$$

$$\left.+\frac{2A}{N_0}\int_0^{T_s}y(t)\sqrt{2}\cos\omega_c t\,dt\sin\Phi_i\right\}, \tag{4.63}$$

где K — не зависит от Φ_i. Если $P(\Phi_i)$ также не зависит от i, то апостериорная вероятность $P[\Phi_i|y(t)]$ максимизируется на таком Φ_i, для которого величина

$$X\cos\Phi_i+Y\sin\Phi_i \tag{4.64}$$

достигает максимума, где

$$X=\frac{1}{AT_s}\int_0^{T_s}y(t)\sqrt{2}\sin\omega_c t\,dt \quad \text{и} \quad Y=\frac{1}{AT_s}\int_0^{T_s}y(t)\sqrt{2}\cos\omega_c t\,dt.$$

Полагая $X=M\cos\Phi$ и $Y=M\sin\Phi$ ($\Phi=\operatorname{arctg}Y/X$), находим, что апостериорная вероятность максимизируется таким Φ_i, которое минимизирует значение $|\Phi-\Phi_i|$, так как $X\cos\Phi_i+Y\sin\Phi_i=M\cos(\Phi-\Phi_i)$ максимально, когда аргумент косинуса минимален по модулю 2π.

В силу того что имеются N сигналов, равноотстоящих по фазе, ошибка при приеме не будет происходить тогда и только тогда, когда разность θ_e между Φ и истинным значением фазы Φ_r принятого сигнала ограничена по абсолютной величине значением

π/N. Если $|\theta_e|$ больше, чем это значение, то разность $|\Phi-\Phi_{r+1}|$ или разность $|\Phi-\Phi_{r-1}|$ будет меньше, чем $|\Phi-\Phi_r|$, и в качестве принятого символа будет выбран некоторый другой символ. Следовательно,

$$P_e(N) = 1 - \int\limits_{-\pi/N}^{\pi/N} p(\theta_e)\, d\theta_e, \tag{4.65}$$

где $p(\theta_e)$ определяется равенством (3.65).

Эту вероятность легко оценить. Заметим сначала, что согласно (4.65) вероятность ошибки не зависит от переданного сигнала. При заданном отношении сигнал/шум она зависит только от числа равноотстоящих фазовых углов. Более того, вероятность ошибки не меняется, если в качестве множества возможных фаз сигнала использовать $\{\Phi'_i\}$ вместо $\{\Phi_i\}$, где

$$\Phi'_i = \left(i - \frac{1}{2}\right)\frac{2\pi}{N}, \quad i = 0, 1, \ldots, N-1. \tag{4.66}$$

Теперь, если передается Φ'_0 и если Y положительна, то ошибка обязательно произойдет. Действительно, если $Y>0$, $0<\Phi<\pi$, то некоторая другая фаза Φ'_i будет ближе к Φ, чем Φ'_0. Таким образом,

$$P_e(N) \geqslant \Pr\{Y > 0 \mid \Phi'_0\} = \Pr\left\{\frac{\pi}{N} < \Phi < \frac{N+1}{N}\pi \mid \Phi_0\right\}. \tag{4.67}$$

Но, кроме того,

$$P_e(N) = \Pr\left\{\frac{\pi}{N} < \Phi < \pi \mid \Phi_0\right\} + \Pr\left\{-\frac{\pi}{N} > \Phi > +\pi \mid \Phi_0\right\} \leqslant$$

$$\leqslant \Pr\left\{\frac{\pi}{N} < \Phi < \frac{N+1}{N}\pi \mid \Phi_0\right\} + \Pr\left\{-\frac{\pi}{N} > \Phi > -\frac{N+1}{N}\pi \mid \Phi_0\right\},$$

и, следовательно, в силу симметрии

$$P_e(N) \leqslant 2\Pr\left\{\frac{\pi}{N} < \Phi < \frac{N+1}{N}\pi \mid \Phi_0\right\} = 2\Pr\{Y > 0 \mid \Phi'_0\}. \tag{4.68}$$

Так как Y — гауссовская случайная величина со средним $E\{Y|\Phi'_0\} = -\sin(\pi/N)$ и дисперсией $\operatorname{var}\{Y|\Phi'_0\} = N_0/2\mathscr{E} \triangleq 1/2R$, то

$$\Pr\{Y > 0 \mid \Phi'_0\} = \frac{1}{2}\left[1 - \operatorname{erf}\left(R^{1/2}\sin\frac{\pi}{N}\right)\right]; \tag{4.69}$$

$$\frac{1}{2}\left[1 - \operatorname{erf}\left(R^{1/2}\sin\frac{\pi}{N}\right)\right] \leqslant P_e(N) \leqslant 1 - \operatorname{erf}\left(R^{1/2}\sin\frac{\pi}{N}\right). \tag{4.70}$$

Вероятность ошибки в этом случае оценивается намного точнее, чем это можно сделать, используя методы § 4.2 [см. неравенство (4.20)].

Если N велико, то, чтобы вероятность $P_e(N)$ была мала, величина $R_b = R/\log_2 N$ должна быть порядка $N^2/\pi^2 \log_2 N$. Следовательно квантованная ФТ в общем случае сравнима с системами модуляции, которые обсуждались ранее, только тогда, когда N относительно мало.

Приведенные выше аргументы можно использовать при определении точного выражения для вероятности ошибки в важном случае, когда $N=2$; в этом случае в действительности достигается нижняя граница P_e. Так, если $\Phi'_0=-\pi/2=3\pi/2$, то ошибка будет происходить тогда и *только тогда,* когда Y положительно. Если Y отрицательно, $\pi<\Phi<2\pi$ и $|\Phi-(3\pi/2)|$ будет наверняка меньше, чем $|\Phi-(\pi/2)|$. Следовательно, если $N=2$, то

$$P_e(2)=\frac{1}{2}\left[1-\mathrm{erf}\left(R^{1/2}\right)\right], \tag{4.71}$$

что подтверждает полученные ранее выводы относительно биортогонального множества символов.

4.6. Фазовая манипуляция. Относительный когерентный прием

Очевидно, что передача с помощью обычной ФТ невозможна без опорной фазы, так как информация фактически содержится в фазе принимаемого сигнала. Вместе с тем, если бы информация содержалась не в самой фазе, а в разности фаз последовательных символов, то необходимость в опорной фазе отпала бы. В этом случае необходимо лишь предположить, что случайная фаза принимаемого сигнала остается строго постоянной в течение интервала $2T_s$ секунд, и тогда можно извлечь информацию из принимаемой последовательности символов. А именно, если символ $s_{i_1}(t)=\sqrt{2}\sin(\omega_c t+i_1(2\pi/N)+\alpha)$ передается на интервале $0<t<T_s$, а $s_{i_2}(t-T_s)=\sqrt{2}\sin(\omega_c(t-T_s)+i_2(2\pi/N)+\alpha)$ — на интервале $T_s<t<2T_s$, и если абсолютное значение изменения α на интервале T_s секунд мало по сравнению с π/N радианами, то влияние этого изменения на вероятность ошибочного решения относительно разности фаз $(i_1-i_2)(2\pi/N)$ будет пренебрежимо малым. Система связи, которая использует разность фаз последовательных ФТ символов, называется *относительной когерентной ФТ* или *ОФТ* системой.

Чтобы найти вид оптимального (по апостериорной вероятности) когерентного приемника для относительного приема, воспользуемся обычной формулой Байеса:

$$P[i_1,\ i_2 \mid y(t),\ \alpha]=\frac{p(y(t)\mid i_1,\ i_2,\ \alpha)\,P(i_1,\ i_2\mid\alpha)}{p(y(t)\mid\alpha)}, \tag{4.72}$$

где i_1 обозначает символ, принятый на интервале времени $0<t<T_s$; i_2 — символ, принятый на интервале $T_s<t<2T_s$, и $y(t)$ — принятый сигнал, искаженный шумом на интервале $0<t<2T_s$. При обычном предположении, что вероятность $P(i_1,\ i_2)$ не зависит от конкретных значений символов i_1 и i_2, оптимальное решение состоит в выборе пары символов i_1, i_2, максимизирующих функцию правдоподобия

$$p[y(t)\mid i_1,\ i_2]=\int\limits_0^{2\pi}p(n_1(t),\ n_2(t)\mid\alpha)\,p(\alpha)\,d\alpha, \tag{4.73}$$

где $p(\alpha)=1/2\pi$, $0\leqslant\alpha<2\pi$. Как обычно, предполагается, что функции $n_1(t)=y_1(t)-s_{i_1}(t)$, $0<t<T_s$ и $n_2(t)=y(t)-s_{i_2}(t)$, $T_s<t<2T_s$ — белые гауссовские случайные процессы, а так как они расположены на непересекающихся интервалах времени, то они независимы. В результате получим

$$p[y(t)\mid i_1,\ i_2]=\frac{K}{2\pi}\int\limits_0^{2\pi}\exp\left\{\frac{2A}{N_0}\left[\int\limits_0^{T_s}y(t)\sqrt{2}\sin\left(\omega_c t+i_1\frac{2\pi}{N}+\alpha\right)dt+\right.\right.$$

$$\left.\left.+\int\limits_{T_s}^{2T_s}y(t)\sqrt{2}\sin\left(\omega_c t+i_2\frac{2\pi}{N}+\alpha\right)dt\right]\right\}d\alpha. \tag{4.74}$$

С этим интегралом мы уже сталкивались несколько раз; поступая как в § 4.3, находим

$$p[y(t)\mid i_1,\ i_2]=\frac{K}{2\pi}\int\limits_{i_1(2\pi/N)}^{2\pi+i_1(2\pi/N)}\exp\{2R[X\cos\Phi+Y\sin\Phi]\}d\,\Phi=$$

$$=KI_0\left[2R(X^2+Y^2)^{1/2}\right], \tag{4.75}$$

где

$$X=\frac{1}{AT_s}\int\limits_0^{T_s}y(t)\sqrt{2}\sin\omega_c t dt+\frac{1}{AT_s}\int\limits_{T_s}^{2T_s}y(t)\sqrt{2}\sin\left(\omega_c t+i\,\frac{2\pi}{N}\right)dt;$$

$$Y=\frac{1}{AT_s}\int\limits_0^{T_s}y(t)\sqrt{2}\cos\omega_c t dt+\frac{1}{AT_s}\int\limits_{T_s}^{2T_s}y(t)\sqrt{2}\cos\left(\omega_c t+i\,\frac{2\pi}{N}\right)dt$$

и $\Phi=\alpha+i_1 2\pi/N$; $i=i_2-i_1$.

В силу того, что $I_0(x)$ — монотонно возрастающая функция x, оптимальное решение состоит в выборе такого значения $i=i_2-i_1$, которое максимизирует величину X^2+Y^2.

Записывая

$$X=x_1+x_2\cos i\,\frac{2\pi}{N}+y_2\sin i\,\frac{2\pi}{N};$$

$$Y=y_1-x_2\sin i\,\frac{2\pi}{N}+y_2\cos i\,\frac{2\pi}{N}, \tag{4.76}$$

где

$$x_j=\frac{1}{AT_s}\int\limits_{(j-1)T_s}^{jT_s}y(t)\sqrt{2}\sin\omega_c t dt;\quad y_j=\frac{1}{AT_s}\int\limits_{(j-1)T_s}^{jT_s}y(t)\sqrt{2}\cos\omega_c t dt,$$

получаем

$$X^2+Y^2=x_1^2+y_1^2+x_2^2+y_2^2+2(x_1x_2+y_1y_2)\cos\frac{2\pi i}{N}+$$

$$+2(x_1y_2-x_2y_1)\sin\frac{2\pi i}{N}. \tag{4.77}$$

Полагая $x_1x_2+y_1y_2=M\cos\Phi$ и $x_1y_2-x_2y_1=M\sin\Phi$, находим аналогично результату, полученному в случае когерентного приема, что оптимальное относительно разности фаз $\Delta\Phi=(2\pi/N)\times\times(i_2-i_1)=\Phi_2-\Phi_1$ решение состоит в выборе $\widehat{\Delta\Phi}$, которая минимизирует значение $|\Phi-\widehat{\Delta\Phi}|$. Заметим также, что оценка максимального правдоподобия величины $\Phi_1\triangleq\alpha+i_1(2\pi/N)$ при заданном сигнале $y(t)$ имеет вид $\hat{\Phi}_1=\operatorname{arctg}(y_1/x_1)$, а оценка максимального правдоподобия величины $\Phi_2=\alpha+i_2(2\pi/N)$ при заданном $y(t)$ — вид $\hat{\Phi}_2=\operatorname{arctg}(y_2/x_2)$. Но

$$\operatorname{tg}(\hat{\Phi}_2-\hat{\Phi}_1)=\frac{\operatorname{tg}\hat{\Phi}_2-\operatorname{tg}\hat{\Phi}_1}{1+\operatorname{tg}\hat{\Phi}_1\operatorname{tg}\hat{\Phi}_2}=\frac{y_2x_1-x_2y_1}{x_1x_2+y_1y_2}=\operatorname{tg}\Phi. \tag{4.78}$$

Следовательно, доказан следующий, согласующийся с интуицией, результат: оптимальный приемник разности фаз $\Delta\Phi$ выбирает значение $\widehat{\Delta\Phi}$, которое минимизирует разность

$$|\widehat{\Delta\Phi}-(\hat{\Phi}_2-\hat{\Phi}_1)|, \tag{4.79}$$

где $\hat{\Phi}_2$ и $\hat{\Phi}_1$ — оптимальные оценки фаз принятых символов $s_{i_2}(t)$ и $s_{i_1}(t)$ соответственно.

Однако приемник, получаемый с учетом этого последнего замечания, в некотором отношении является более сложным, чем это необходимо. Более удобная практическая реализация приведена на рис. 4.5; в ней используется тот факт, что оптимальное решение требует знания только двух статистик $x_1x_2+y_1y_2$ и $x_1y_2-x_2y_1$ [см. (4.77)]. Первая из этих статистик вырабатывается на выходе верхнего фильтра на рис. 4.5 [ср. с ф-лой (4.30)], а вторая — на выходе нижнего фильтра. (Здесь ω_cT_s, по предположению, равно четному целому числу, умноженному на π.) Устройство, выносящее реше-

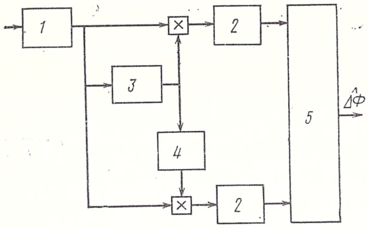


Рис. 4.5. Функциональная схема демодулятора относительной когерентной ФТ:

1 — некогерентный согласованный фильтр; 2 — фильтр нижних частот; 3 — задержка на T_s, с; 4 — поворот фазы на 90°; 5 — устройство, выносящее решения

ния, взвешивает эти выходы в моменты выборок $t=iT_s$ в соответствии с равенством (4.77). В двоичном случае ($N=2$) этот приемник становится еще проще, так как нужна лишь верхняя статистика, определяемая верхним фильтром, а решение зависит только от знака этого выражения.

Определение границ вероятности ошибки P_e в этом случае затруднительно. Можно подсчитать плотность распределения разности фаз $\hat{\Phi}_2-\hat{\Phi}_1$, но результирующее выражение будет громоздким. Вместо этого ниже получено приближенное выражение для P_e. Ошибка $\theta_{e1}=\Phi_1-\hat{\Phi}_1$ в оценке величины Φ_1 [фазы символа $s_{i_1}(t)$] задается равенством [ср. с ф-лой (3.65)]

$$p(\theta_{e1})=\frac{e^{-R}}{2\pi}+\frac{(2R)^{1/2}}{2\pi}\cos\theta_{e1}\,e^{-R\sin^2\theta_{e1}}\int\limits_{-\infty}^{(2R)^{1/2}\cos\theta_{e1}}\exp\left(-\frac{x^2}{2}\right)dx\approx$$

$$\approx\frac{(2R)^{1/2}}{\sqrt{2\pi}}\cos\theta_{e1}\exp\left(-R\sin^2\theta_{e1}\right),\qquad(4.80)$$

где опять $R=(A^2T_s/N_0)$. Можно возразить, что это последнее приближение в действительности является нижней границей для $p(\theta_{e1})$ при $|\theta_{e1}|\leqslant(\pi/N)$. Во всяком случае, чтобы система имела приемлемые характеристики, величина $|\theta_{e1}|$ должна с большой вероятностью быть меньше, чем π/N, а потому $(2R)^{1/2}\cos\theta_{e1}$ в общем случае велико по сравнению с единицей, так что это приближение имеет разумную точность. Аналогично, полагая $\theta_{e2}=\Phi_2-\hat{\Phi}_2$, где Φ_2 — фаза символа $s_{i_2}(t)$, а $\hat{\Phi}_2$ — ее оптимальная оценка, получаем

$$p(\theta_{e2})\approx\frac{(2R)^{1/2}}{\sqrt{2\pi}}\cos\theta_{e2}\exp\left(-R\sin^2\theta_{e2}\right).\qquad(4.81)$$

Решение относительно $\Delta\Phi$ будет верным тогда и только тогда, когда $|\theta_{e2}-\theta_{e1}|$ меньше, чем $2\pi/2N$, и только в этом случае функция $|\hat{\Delta}\Phi-(\hat{\Phi}_2-\hat{\Phi}_1)|=|\hat{\Delta}\Phi-\Delta\Phi+\theta_{e2}+\theta_{e1}|$ будет достигать минимума при $\hat{\Delta}\Phi=\Delta\Phi$. Более того, так как θ_{e1} и θ_{e2} должны быть малыми, если выносится правильное решение, то $|\sin(\theta_{e2}-\theta_{e1})|=|\sin\theta_{e2}\cos\theta_{e1}-\sin\theta_{e1}\cos\theta_{e2}|\approx|\sin\theta_{e2}-\sin\theta_{e1}|$. Поэтому

$$P_e(N)=1-\Pr\left\{|\theta_{e2}-\theta_{e1}|<\frac{\pi}{N}\right\}\approx1-\Pr\left\{|\sin(\theta_{e2}-\theta_{e1})|<\sin\frac{\pi}{N}\right\}\approx$$

$$\approx1-\Pr\left\{|\sin\theta_{e2}-\sin\theta_{e1}|<\sin\frac{\pi}{N}\right\}.\qquad(4.82)$$

Но $p(\alpha=\sin\theta_{e1})\approx\dfrac{(2R)^{1/2}}{\sqrt{2\pi}}\exp(-R\alpha^2)$ и $p(\beta=\sin\theta_{e2})\approx\dfrac{(2R)^{1/2}}{\sqrt{2\pi}}\times\exp(-R\beta^2)$, так что как α, так и β приближенно имеют гауссовские распределения с нулевыми средними и дисперсией $1/2R$. В силу того, что α и β — независимые гауссовские величины, их разность также гауссовская случайная величина с $E(\alpha-\beta)=E(\alpha)-E(\beta)=0$ и $\operatorname{var}(\alpha-\beta)=E(\alpha^2)+E(\beta^2)=1/R$. Таким образом,

$$P_e(N)\approx 1-\Pr\left\{|\alpha-\beta|<\sin\frac{\pi}{N}\right\}=$$

$$=1-\frac{(R)^{1/2}}{\sqrt{2\pi}}\int\limits_{-\sin(\pi/N)}^{\sin(\pi/N)}\exp\left(-\frac{R}{2}\gamma^2\right)d\gamma=1-\operatorname{erf}\left\{\left(\frac{R}{2}\right)^{1/2}\sin\frac{\pi}{N}\right\}. \qquad (4.83)$$

Сравнение равенств (4.70) и (4.83) показывает, что вероятность ошибки для относительного когерентного приема, по существу, равна вероятности при когерентном приеме, если отношение энергии сигнала к спектральной плотности шума в последнем случае уменьшить вдвое.

Справедливость этого выражения для вероятности ошибки очень сильно зависит от приближения в равенстве (4.82). Это приближение, в свою очередь, зависит от предположения, что $R\cos\theta_e$ велико. Для больших значений N условие $|\theta_{e1}-\theta_{e2}|<\pi/N$ достаточно для того, чтобы θ_{e1} и θ_{e2} были малыми и чтобы необходимые предположения удовлетворялись. Таким образом, следует ожидать, что оценка вероятности ошибки, полученная здесь, будет иметь смысл для достаточно больших N. В важном случае, когда $N=2$, точность этого выражения сомнительна.

К счастью, другой способ приводит к выводу точной формулы для вероятности ошибки, когда $N=2$. В этом случае имеются лишь два возможных символа: $s_1(t)=\sqrt{2}\sin\omega_c t$ и $s_2(t)=-s_1(t)$. Для определения разности фаз между двумя последовательными символами требуется различить лишь два события: либо на интервале $(0,\ T_s)$ был принят сигнал $s_i(t)$, а на интервале $(T_s,\ 2T_s)$ — сигнал $s_i(t-T_s)$, либо был принят сигнал $s_i(t)$, а затем сигнал $-s_i(t-T_s)$. Ситуации одинаковы как при $i=1$, так и при $i=2$, так как не ставится целью определить i. Независимо от i, следовательно, необходимо лишь различить два «расширенных символа»: $u_1(t)=s_i(t)$, $s_i(t-T_s)$ (случай, когда два одинаковых символа $s_i(t)$ следуют друг за другом) и $u_2(t)=s_i(t)$, $-s_i(t-T_s)$. Решение этой задачи полностью эквивалентно решению в фазовонекогерентной системе относительно того, был ли передан сигнал $u_1(t)$ или $u_2(t)$. Так как $u_1(t)$ и $u_2(t)$, очевидно, взаимно ортогональны и каждый из них имеет удвоенную по сравнению с символами $s_1(t)$ и $s_2(t)$ энергию, то вероятность ошибки согласно ф-ле (4.46) имеет вид

$$P_e(2)=\frac{1}{2}\exp(-R). \qquad (4.84)$$

Если же воспользоваться ф-лой (4.83), то для $N=2$

$$P_e(2)\approx 2e^{-R/2}/\sqrt{2\pi R}, \qquad (4.85)$$

что является довольно неточной оценкой.

4.7. Сравнение вероятностей ошибок в бите, символе и слове

Мерой качества дискретных систем связи, использованной повсюду в этой главе, была вероятность ошибки в символе. Следует иметь в виду, однако, что даже если две системы имеют одну и ту же вероятность ошибки в символе, их характеристики с точки зрения потребителя могут быть совершенно различными. Например, чем большее число битов приходится на символ, тем больше эти ошибки в битах группируются вместе. Если вероятность ошибки в символе равна 10^{-3}, то математическое ожидание числа безошибочных символов между какими-либо двумя ошибочными символами равно 1000. Если каждый символ содержит один бит информации, то математическое ожидание числа битов, разделяющих два ошибочных бита, равно 1000, в то же время математическое ожидание этой величины, когда символ содержит 10 битов, равно 10 000 бит. Естественно, что ошибка в символе, вообще говоря, создает больше ошибок в битах во втором случае, поэтому процент ошибок в битах примерно тот же самый, как мы скоро увидим. Тем не менее эффект группирования может сделать одну систему более предпочтительной перед другой даже при одной и той же частоте ошибок в символах. Какая из них предпочтительнее, зависит от конкретной ситуации.

Одной из довольно часто встречающихся альтернатив меры качества для дискретных систем является вероятность ошибки в бите, а не ошибки в символе. Но эта мера качества имеет тот же недостаток, что и вероятность ошибки в символе, а именно: она не обязательно является мерой, представляющей наибольший интерес для потребителя. Часто информационные биты могут быть объединены в информационные *слова*, скажем, по k бит каждое. Каждое слово может, например, соответствовать одному наблюдению в эксперименте или одному отсчету данных. Если этот случай имеет место, часто оказывается, что приемлемой мерой качества является вероятность ошибки в информационном *слове*. Потребитель хочет, чтобы принятое слово было правильным; если какой-нибудь бит в слове является ошибочным, информация, представляемая словом, может оказаться бесполезной для потребителя. Нс сравнивать две системы на основе их вероятностей ошибок в слове довольно непрактично, так как результаты сравнения будут различными при различных значениях k (число бит в слове).

Короче говоря, хотя вероятность ошибки в символе может не быть мерой, подходящей какому-то потребителю, но и любая другая мера будет подходящей лишь для некоторых конкретных ситуаций. К счастью, каждая из альтернативных мер качества, упомянутых выше, т. е. вероятность ошибки в бите и вероятность ошибки в слове, могут быть, вообще говоря, довольно просто найдены, исходя из вероятности ошибки в символе.

Ниже эти вопросы рассматриваются подробнее.

1. Вероятности ошибки в бите; множества символов с равными коэффициентами взаимной корреляции ($\rho_{ij}=\rho$). Для того чтобы выразить вероятность ошибки в бите P_b через вероятность ошибки в символе P_e в системе связи с N символами, в которой коэффициенты взаимной корреляции $\rho_{ij}=\rho$ при всех i, j, $i\neq j$, нужно лишь учесть, что вероятность того, что какой-либо символ перейдет в какой-либо другой символ, не зависит от того, какие конкретные символы рассматриваются. Тогда при условии, что произошла ошибка в символе, переданная двоичная n-последовательность ($n=\log_2 N$) с равной вероятностью переходит в любую из 2^n-1 возможных других n-последовательностей. Так как число n-последовательностей, отличающихся от данной n-последовательности в точности в i битах, равно $\binom{n}{i}$, то математическое ожидание доли n битов, которая будет ошибочной при условии, что символ является ошибочным, равно:

$$\eta_b=E\ (\text{доля ошибочных битов}\,|\,\text{ошибка в символе}) =$$

$$=\frac{1}{2^n-1}\sum_{i=1}^{n}\frac{i}{n}\binom{n}{i}=\frac{2^{n-1}}{2^n-1}; \tag{4.86}$$

$$P_b=\eta_b P_e=\frac{N}{2(N-1)}P_e\approx\frac{1}{2}P_e. \tag{4.87}$$

2. Вероятности ошибки в бите; множества биортогональных символов. Обозначая через P_{e1} вероятность перехода некоторого символа в некоторый другой заданный символ, отличный от дополнения к первоначальному, через P_{e2} — вероятность перехода некоторого символа в его дополнение и через P_e — вероятность ошибки в символе, получим

$$P_e=(N-2)P_{e1}+P_{e2}. \tag{4.88}$$

Так как $P_{e2}<P_{e1}$, то математическое ожидание числа ошибочных битов, очевидно, принимает минимальное значение, когда дополнительные n-последовательности представляются дополнительными символами. В этом случае

$$P_b=P_{e1}\sum_{i=1}^{n-1}\frac{i}{n}\binom{n}{i}+P_{e2}=\left(2^{n-1}-1\right)P_{e1}+P_{e2}=\frac{1}{2}(P_e+P_{e2})\approx P_e/2. \tag{4.89}$$

Приближение в последнем равенстве ф-лы (4.89) справедливо всегда, кроме случая малых значений N. Если $N=2$, то $P_e=P_{e2}$ и P_b равно P_e, а не $P_e/2$. Интересно, что вероятности ошибки в бите, когда $N=2$ и $N=4$ одинаковы, если только два множества символов имеют одну и ту же энергию сигнала на бит. Чтобы убедиться в этом, обозначим через x выход фильтра, согласованного с одним из $N=2$ биортогональных символов, а через x_1 и x_2 — выходы фильтров, согласованных с двумя из ортогональных символов биортогонального множества с $N=4$. Предположим, что отображение является таким, что, когда $x_1>|x_2|$, принятый символ отождествляется с сообщением 00, а когда $x_2>|x_1|$, он отождествляется с 01. Если передается символ 00, то ошибка в первом бите происходит тогда и только тогда, когда $x_1+x_2\leqslant 0$, так как если сумма x_1+x_2 положительна, то либо $x_1>|x_2|$, либо $x_2>|x_1|$. Таким образом, вероятность ошибки в бите (в силу симметрии она одинакова для каждого из двух битов) является вероятностью события $y \triangleq (x_1+x_2)/2\leqslant 0$. Но так как x и y — гауссовские величины с $E(y|00)=\frac{1}{2}E(x_1|00)=E(x|0)$ и $\operatorname{var}(y)=\frac{1}{4}\operatorname{var}(x_1)+\frac{1}{4}\operatorname{var}(x_2)=$ $=\frac{1}{2}\operatorname{var}(x_1)=\operatorname{var}(x)$, то $\Pr(y<0|00)=\Pr(x\leqslant 0|0)$, и вероятности ошибки в бите в этих двух случаях совпадают.

3. Вероятности ошибки в бите; ФТ символы. В этом случае вероятность перехода символа в какой-либо из двух «ближайших» (по фазе) символов, очевидно, много больше (если вероятность ошибки в символе достаточно мала), чем вероятность какой-либо ошибки другого вида. Отображая двоичные n-последовательности в символы таким образом, чтобы пара n-последовательностей, соответствующих каким-либо двум смежным символам, отличалась от каждой из остальных лишь в одной двоичной позиции, можно добиться того, чтобы наиболее вероятное число ошибок в битах при условии ошибки в символе было просто равно единице. При таком отображении

$$P_b \approx P_e/\log_2 N. \tag{4.90}$$

Отображение, удовлетворяющее ограничению, описанному в предыдущем абзаце, называется *кодом Грэя*. Существование кодов Грэя n-последовательностей для всех целых n легко установить методом индукции. Пусть $g_1, g_2, \ldots, g_N$ такое упорядочение двоичных n-последовательностей, что g_i и g_{i+1} отличаются лишь одним битом для всех $i=1, 2, \ldots, N$ $(N+1\equiv 1)$. Далее пусть νg_i обозначает $(n+1)$последовательность, получаемую с помощью прибавления двоичного символа ν в качестве префикса к g_i. Тогда ясно, что $0g_1, 0g_2, \ldots, 0g_N, 1g_N, 1g_{N-1}, \ldots, 1g_2, 1g_1$ является упорядочением $(n+1)$-последовательностей, удовлетворяющим тому же ограничению. Так как последовательность *0,1* представляет такое упорядочение для $n=1$, то коды Грэя существуют для всех n.

4. Вероятности ошибок в слове. Если k бит образуют слово и если для представления каждого бита используется один символ, то вероятность ошибки в слове

$$P_w = 1-(1-P_e)^k, \tag{4.91}$$

где P_e — вероятность ошибки в символе. На рис. 4.6 сравниваются вероятности ошибки в слове, когда: 1) каждый бит пятибитового информационного слова передается как биортогональный символ; 2) когда каждое слово передается как один из 32 биортогональных символов.

По-видимому, наиболее важный вывод, который можно сделать при сравнении вероятности ошибки в слове с вероятностями ошибок в бите или символе, вытекает из поведения этих вероятностей при малых отношениях сигнал/шум R. Используя какую-либо одну из последних двух мер качества, находим, что для достаточно малых значений R лучше использовать по возможности меньшее число символов. Это положение быстро меняется, однако, с ростом R. Если же рассматриваются вероятности ошибки в слове, то в противоположность этому всегда лучше использовать символ для того, чтобы представить слово, а не бит (ср. с рис. 4.6).

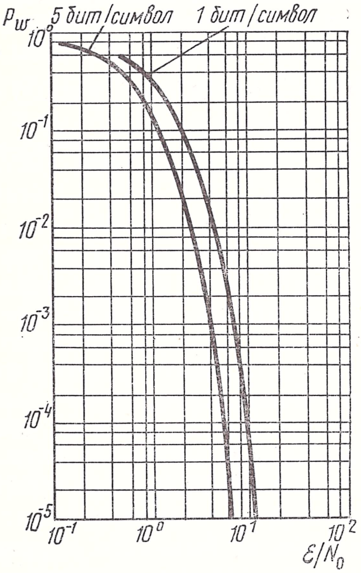


Рис. 4.6. Сравнение вероятностей ошибок, приходящихся на слово ($k=5$)

Это свойство довольно легко объяснить. Если рассматривается вероятность ошибки в слове, то в качестве меры качества представляет интерес вероятность перехода сигнала, представляющего одно слово, в какой-либо сигнал, представляющий некоторое другое слово, независимо от числа битов, соответствующих каждому символу. Если же каждый бит индивидуально представляется с помощью, например, одного трансортогонального символа ($\rho_{12}=-1$) и k битов составляют слово, то корреляция между двумя сигналами (представляющими слова) изменяется от $\rho_{ij}=(k-2)/k$ до -1. Но в когерентной системе трансортогональные коды, имеющие $\rho_{ij}=-1/(2^k-1)$ для всех i и j при $i\neq j$, по-видимому, оптимальны при всех значениях R (ср. с § 4.2). Поэтому должно проявляться преимущество отображения слов перед отображением отдельных битов в трансортогональные символы. Так как характеристики множеств ортогональных и биортогональных символов близки к характеристикам трансортогональных множеств, то следует ожидать, что те же выводы справедливы и для ранее рассмотренных алфавитов.

Наконец, когда l слов отображаются одним символом, вероятность ошибки в слове может быть выражена через вероятности ошибок в символе аналогично тому, как это было сделано при получении вероятностей ошибок в бите, выраженных через вероятности ошибок в символе. В качестве примера предположим, что пара слов, содержащих k битов каждое, должна быть передана в виде одного из 2^{2k} ортогональных символов. Математическое ожидание доли ошибочных слов при условии, что произошла ошибка в символе, имеет вид

$$\eta_{\omega} = \frac{1}{2}\,\text{Pr (первое слово правильное и второе слово ошибочное)} +$$

$$+ \frac{1}{2}\,\text{Pr (второе слово правильное и первое слово ошибочное)} + \text{Pr (оба слова}$$

$$\text{ошибочны)} = \frac{2^k - 1}{2^{2k} - 1} + \frac{2^{2k} - 1 - 2(2^k - 1)}{2^{2k} - 1} = \frac{2^k}{2^k + 1}\,. \qquad (4.92)$$

Следовательно,

$$P_{\omega} = \frac{2^k}{2^k + 1}\, P_e. \qquad (4.93)$$

4.8. Заключительные замечания

Вероятность ошибочного приема в системе передачи, использующей N символов равной энергии и канал с белым гауссовским шумом, является функцией лишь уровней сигнала и шума на выходах фильтров приемника и корреляции (понимаемой как в когерентном, так и в некогерентном смыслах) между этими различными выходами. Следовательно, замечания, аналогичные сделанным в § 3.8, в равной мере уместны и здесь при соблюдении тех же общих условий. В частности, не существенны конкретные виды сигналов, используемые в рассматриваемой здесь системе связи; все алфавиты символов, имеющие одно и то же множество коэффициентов корреляции, являются одинаково хорошими, если они используются при одних и тех же уровнях сигнала и шума. Более того, анализ характеристик, проведенный в этой главе, применим не только к оптимальным приемникам. Результаты легко могут быть распространены на приемники, отличные от приемников с согласованными фильтрами, если можно определить уровни сигнала и шума на выходе и корреляцию между этими различными выходами. Однако результаты, полученные при использовании согласованных фильтров, дают нижние границы для вероятности ошибки, достижимой при использовании какого-либо другого множества фильтров.

Системы связи, рассмотренные здесь и в предыдущей главе, служат основой при последующем рассмотрении проблем синхронизации. Это вовсе не означает, что это рассмотрение охватывает все интересные системы связи. На самом деле некоторые очевидные варианты (например, дискретно-амплитудная АИМ, непрерывно-амплитудная ВИМ, частотная манипуляция и когерентная относительная ФТ) и гибриды этих систем (например, АИМ-ФТ) сразу же напрашиваются сами собой. Тем не менее рассмотренные системы являются достаточно представительными, чтобы дать возможность обсудить вопросы синхронизации в достаточно общей постановке.

Задачи

4.1. а) Предположим, что принимается сигнал $\sqrt{2}\gamma\xi(t)\sin(\omega_c t+\Phi)+n(t)$, $0\leqslant t\leqslant T_s$, где $\xi(t)$ — один из двух равновероятных ортогональных сигналов равной энергии, а $n(t)$ — белый гауссовский шум. Фаза несущей — случайная величина, равномерно распределенная на интервале $(0, 2\pi)$, а амплитуда сигнала γ — случайная величина с релеевским распределением $p(\gamma)=2\gamma e^{-\gamma^2}$, $\gamma\geqslant 0$. (Если такие характеристики случайной амплитуды и фазы возникают вследствие влияния канала, то он называется каналом с *релеевскими замираниями* или *многолучевым* каналом. Такой канал возникает, например, когда энергия сигнала переносится большим числом лучей с примерно одинаковыми затуханиями, но меняющимися задержками в разных лучах. Если γ и Φ могут считаться постоянными на протяжении каждого символа, как здесь предполагается, говорят, что замирания являются медленными.)

Показать, что минимальная достижимая вероятность ошибки в символе равна $P_e=1/(2+\overline{R})$, где $\overline{R}$ — отношение средней принятой энергии на символ к спектральной плотности шума.

б) Предположим теперь, что принимаемый сигнал имеет вид $\sqrt{2}\xi(t)\sin\omega_c t+$ $+\sqrt{2}\gamma\xi(t)\sin(\omega_c t+\Phi)+n(t)$ с теми же обозначениями, что и ранее. (Первое слагаемое, называемое *спектральной* компонентой, может возникать, если один из лучей намного превосходит все остальные.) Показать, что если использовать для этого сигнала тот же приемник, который был использован в п. а) этой задачи, то вероятность ошибки будет $P'_e=P_e\exp\{-P_eR_s\}$, где P_e определяется, как и в п. а), а R_s — отношение энергии спектральной компоненты к спектральной плотности шума.

в) Описать оптимальный приемник для сигнала, определенного в п. б).

4.2. Показать, что вероятность $P_e(N)$, определенная равенством (4.8), удовлетворяет неравенствам:

$$\frac{1}{2}\left\{1-\operatorname{erf}\left(\frac{\overline{R}^*}{2}\right)^{1/2}\right\}\leqslant P_e(N)\leqslant\frac{N-1}{2}\left\{1-\operatorname{erf}\left(\frac{R^{**}}{2}\right)^{1/2}\right\},$$

где $\overline{R}^*=R\times$ $\times\left\{\frac{1}{N}\sum_{r=1}^{N}(1-\rho_r)^{1/2}\right\}^2$; $R^{**}=\min\limits_{r}R(1-\rho_r)$ и $\rho_r=\min\limits_{\substack{i\\ i\neq r}}(1-\rho_{ir})$ [ср. с неравенством (4.19)].

Глава 5

ОПТИМАЛЬНЫЕ ФИЛЬТРЫ, СОГЛАСОВАННЫЕ ФИЛЬТРЫ И СИСТЕМЫ ФАЗОВОЙ АВТОПОДСТРОЙКИ ЧАСТОТЫ

5.1. Введение

Задачи, рассмотренные в двух последних главах, в той или иной мере были связаны с извлечением информации из сигнала, искаженного шумом. В каждом случае сигнал представлял собой последовательность функций, каждая из которых, в свою очередь, была функцией одного или бо́льшего числа параметров, которые по предположению оставались неизменными в течение известного интервала времени длины T_s секунд. Задача состояла в определении (с возможно большей точностью) параметра, представляющего интересующую информацию. Это привело к рассмотрению согласованных фильтров и связанных с ними устройств.

Эту главу начнем с исследования вида «оптимального» фильтра для намного более общего класса сигналов. А именно, принимаемый сигнал представляет собой выборочную функцию произвольного стационарного в широком смысле случайного процесса, описываемого лишь с помощью автокорреляционной функции (или, что эквивалентно, с помощью спектральной плотности мощности). Пусть входом фильтра (наблюдаемыми) будет процесс $y(t)$. [В общем случае $y(t)$ имеет вид $y(t)=x(t)+n(t)$, где $x(t)$ представляет собой информацию, а $n(t)$ обозначает шум]. Обозначим выход фильтра через $\hat{z}(t)$, а желаемый сигнал — через $z(t)$. Тогда оптимальный фильтр определяется как фильтр, который дает наилучшее приближение в смысле среднеквадратической ошибки к желаемому сигналу $z(t)$, т. е. оптимальный фильтр выбирается так, чтобы минимизировать ошибку

$$\sigma_e^2 = E\,[\hat{z}(t) - z(t)]^2. \tag{5.1}$$

Предполагается, что случайные процессы $y(t)$ и $z(t)$ стационарны, а параметры фильтра не зависят от времени, так что ошибка $\sigma^2{}_e$ тоже не зависит от времени.

Для того чтобы определить структуру оптимального фильтра, обычно необходимо ввести ограничения на класс рассматриваемых устройств. Предположим, что фильтр линейный, так что $\hat{z}(t)$ будет линейной функцией наблюдаемых $y(t)$. Это ограничение имеет двойное преимущество: оно не только приводит к относительно простой процедуре оптимизации, но также позволяет физически реализовать устройство (или, по крайней мере, получить хорошее приближение). Частотная характеристика оптимального линейного фильтра будет получена в следующем параграфе.

Следует указать, что некоторые другие критерии ошибок, отличные от среднеквадратической ошибки, также могут быть удовлетворительными, а в некоторых ситуациях и более адекватными. Средняя абсолютная ошибка

$$e_a = E\,|\hat{z}(t) - z(t)| \qquad (5.2$$

или максимум абсолютной ошибки

$$e_M = \max_t |\hat{z}(t) - z(t)| \qquad (5.3)$$

могут представлять, например, больший интерес для потребителя, чем среднеквадратическая ошибка. Важна также средняя ошибка

$$\eta = E[\hat{z}(t) - z(t)]. \qquad (5.4)$$

Однако если η отлична от нуля, то нетрудно показать, что среднеквадратическую ошибку можно легко уменьшить. Предположим, что $\hat{z}(t)$ — выход оптимального в смысле среднеквадратической ошибки фильтра, и рассмотрим функцию $\sigma^2_e(a) = E[\hat{z}(t) - a - z(t)]^2 = E[\hat{z}(t) - z(t)]^2 - 2a\eta + a^2$. Так как $\sigma^2_e(a)$ — монотонно возрастающая функция $|a - \eta|$, то можно уменьшить среднеквадратическую ошибку, вычитая из выходного сигнала фильтра постоянную η. Во всех практических случаях при этом оптимальный в среднеквадратическом смысле линейный фильтр обычно не меняется при наложении ограничения также и на среднюю ошибку. Во всех интересных случаях средняя ошибка на выходе такого фильтра фактически равна нулю [1]).

Причина предпочтения критерия среднеквадратической ошибки перед другими состоит, главным образом, в его удобстве. Математические операции не являются громоздкими, а решение задачи можно получить в явном виде; это последнее утверждение не верно, вообще говоря, почти для всех других нетривиальных критериев, которые можно было бы выбрать. Более того, с интуитивной точки зрения среднеквадратическая ошибка — довольно удовлетворительная мера качества. В конце концов, она является «мощностью» или, с точки зрения статистики, дисперсией сигнала ошибки. Наконец, если необходимо дальнейшее обоснование для выбора критерия среднеквадратической ошибки, упомянем, что во многих важных случаях получающийся в результате фильтр является оптимальным с точки зрения значительного более общего класса критериев. После всего сказанного рассматриваемая задача сводится к задаче оценки того типа, который обсуждался в § 2.9. (Как и в предыдущих главах, можно вначале профильтровать принятый сигнал и с помощью теоремы отсчетов свести множество наблюдаемых к дискретному множеству Y, а затем допустить, что полоса частот фильтра становится бесконечной.) Задача состоит в оценке случайной величины $z(t_0)$ в некоторый момент t_0 на основе наблюдаемых $y(t)$, $t_1<t<t_2$. (Обычно в рассматриваемых здесь задача t_1 равно $-\infty$, а $t_2 \leqslant t_0$.) Но, по § 2.9 оптимальная оценка $\hat{z}(t_0)$ величины $z(t_0)$ для широкого класса критериев, включающего в себя критерий среднеквадратической ошибки, имеет вид $\hat{z}(t_0)=E[z(t_0) \mid Y]$. В частности, это справедливо, если стоимость ошибки $e(t_0)=\hat{z}(t_0)-z(t_0)$ является какой-либо монотонной неубывающей функцией $e(t_0)$ и если плотность распределения $p[z(t_0) \mid Y]$ — симметричная унимодальная функция $z(t_0)$. Этот случай возникает, например, когда и $y(t)$, и $z(t)$ — совместно гауссовские случайные процессы. Интересно также отметить, что $E[z(t_0) \mid Y]$ является линейной функцией наблюдаемых $Y=\{y_i\}$, если случайные величины $z(t_0)$, y_1, y_2, ... имеют совместно гауссовское распределение. Таким образом, если $y(t)$ и $z(t)$ совместно гауссовские процессы, ограничение, состоящее в том, что оценка $\hat{z}(t_0)$ должна быть линейной функцией $y(t)$, является излишним. Тот же самый результат получается без этого ограничения для любой стоимостной функции, которая является монотонно неубывающей функцией ошибки $e(t_0)=\hat{z}(t_0)-z(t_0)$.

---

[1]) Это не эквивалентно утверждению, что оценка $\hat{z}(t)$ величины $z(t)$ является несмещенной (см. § 2.9). Скорее математическое ожидание смещения равно нулю. *(Прим. авт.)*.

5.2. Оптимальный линейный фильтр

Оптимальный линейный фильтр, в соответствии с данным выше определением, минимизирует среднеквадратическую разность σ^2_e между некоторым желаемым сигналом $z(t)$ и выходом фильтра $\hat{z}(t)$. Таким образом, требуется найти фильтр с импульсным откликом $h(t)$, для которого величина

$$\sigma_e^2 = E\,[\hat{z}(t)-z(t)]^2 = E\left\{\int_{-\infty}^{\infty} y(t-\tau)\,h(\tau)\,d\tau - z(t)\right\}^2 =$$

$$= R_z(0) - 2\int_{-\infty}^{\infty} R_{yz}(\tau)\,h(\tau)\,d\tau + \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} R_y(\tau-\eta)\,h(\tau)\,h(\eta)\,d\tau\,d\eta \qquad (5.5)$$

достигает своего минимально возможного значения. Через $R_{\alpha\beta}(\tau)$, как обычно, обозначены корреляционные функции $R_{\alpha\beta}(\tau) = E(\alpha(t)\,\beta(t+\tau))$ и $R_\alpha(\tau)=R_{\alpha\alpha}(\tau)$.

Как будет показано, оптимальный фильтр легко найти, если на него не накладываются никакие дополнительные ограничения. Однако, чтобы решение имело какой-нибудь практический смысл, одно ограничение все же должно быть наложено. Оно состоит в том, чтобы фильтр был *физически реализуемым*, т. е. чтобы сигнал на выходе отсутствовал до момента появления сигнала на его входе и, следовательно, чтобы его импульсный отклик $h(t)$ был тождественно равен нулю для всех $t<0$. Хотя это ограничение до некоторой степени усложняет анализ, оптимальный физически реализуемый фильтр может быть найден лишь несколько большими усилиями.

Удобно также в последующих выводах предположить существование частотной характеристики $H(\mathrm{i}\omega)$ оптимального фильтра. Легко видеть, что это предположение справедливо, если фильтр является *устойчивым,* т. е. если каждый ограниченный входной сигнал $x(t)$ вызывает ограниченный выходной сигнал $y(t)$. Чтобы проверить это утверждение, покажем, что фильтр устойчив тогда и только тогда, когда его импульсный отклик абсолютно интегрируем:

$$\int_{-\infty}^{\infty} |h(t)|\,dt < \infty. \tag{5.6}$$

Это условие является достаточным для существования преобразования Фурье $H(\mathrm{i}\omega)$, так как

$$H(\mathrm{i}\,\omega)\,| = \left| \int_{-\infty}^{\infty} h(t)\,\mathrm{e}^{-\mathrm{i}\omega t}\,dt \right| \leqslant \int_{-\infty}^{\infty} |h(t)|\,|\mathrm{e}^{-\mathrm{i}\omega t}|\,dt = \int_{-\infty}^{\infty} |h(t)|\,dt.$$

Чтобы доказать эквивалентность устойчивости фильтра и абсолютной интегрируемости импульсной переходной характеристики, заметим, что

$$|y(t)| = \left| \int_{-\infty}^{\infty} h(\tau)\,x(t-\tau)\,d\tau \right| \leqslant \int_{-\infty}^{\infty} |h(\tau)|\,|x(t-\tau)|\,d\tau$$

и, если $|x(t)| \leqslant X$ для всех t, то $|y(t)| \leqslant X\int_{-\infty}^{\infty} h(\tau)\,d\tau$. Вместе с тем, если для некоторого значения t входной сигнал

$$x(t-\tau) = \operatorname{sgn} h(\tau) = \begin{cases} 1, & h(\tau) > 0; \\ -1, & h(\tau) < 0 \end{cases}$$

для всех τ, то для этого сигнала имеем: $y(t) = \int_{-\infty}^{\infty} |h(\tau)|\,d\tau$, и утверждение доказано.

Нетрудно показать, что импульсный отклик оптимального фильтра удовлетворяет следующему интегральному уравнению, которое называется *уравнением Винера—Хопфа:*

$$\int_{a}^{\infty} h(\tau)\,R_y(\tau-\eta)\,d\tau = R_{yz}(\eta) \tag{5.7}$$

для всех $\eta > a$. Если фильтр должен быть физически реализуемым, то $a=0$; в противном случае $a=-\infty$. Среднеквадратическая ошибка в случае, когда импульсный отклик фильтра удовлетворяет этому уравнению, имеет вид

$$\sigma_e^2 = R_z(0) - \int_a^\infty \int_a^\infty h(\tau) h(\eta) R_y(\tau - \eta)\, d\tau\, d\eta =$$

$$= R_z(0) - \int_a^\infty R_{yz}(\tau) h(\tau)\, d\tau, \tag{5.8}$$

что можно проверить, подставляя ф-лу (5.7) в (5.5).

Для того чтобы доказать оптимальность фильтра, удовлетворяющего ур-нию (5.7), покажем, что разность ошибок $\sigma^2{}_e[g(t)] - \sigma^2{}_e[h(t)]$ неотрицательна; $\sigma^2{}_e[g(t)]$ означает среднеквадратическую ошибку в случае, когда используется произвольный фильтр $g(t)$, а $\sigma^2{}_e[h(t)]$ — аналогичную величину в случае, когда используется фильтр, удовлетворяющий ур-нию (5.7). Если фильтр $h(t)$ должен быть физически реализуемым, то, конечно, таким же должен быть и фильтр $g(t)$. В остальных случаях ограничения на фильтр $g(t)$ не накладываются. Используя (5.5) и (5.8), получаем

$$\sigma_e^2[g(t)] - \sigma_e^2[h(t)] = -2\int_a^\infty g(\tau) R_{yz}(\tau)\, d\tau + \int_a^\infty \int_a^\infty [g(\tau) g(\eta) +$$

$$+ h(\tau) h(\eta)] R_y(\tau - \eta)\, d\tau\, d\eta = -2\int_a^\infty \int_a^\infty g(\tau) h(\eta) R_y(\tau - \eta)\, d\tau\, d\eta +$$

$$+ \int_a^\infty \int_a^\infty [g(\tau) g(\eta) + h(\tau) h(\eta)] R_y(\tau - \eta)\, d\tau\, d\eta =$$

$$= \int_a^\infty \int_a^\infty [g(\tau) - h(\tau)]\, [g(\eta) - h(\eta)] R_y(\tau - \eta)\, d\tau\, d\eta = \tag{5.9}$$

$$= \frac{1}{2\pi} \int_{-\infty}^{\infty} |\, G(\mathrm{i}\,\omega) - H(\mathrm{i}\,\omega)\,|^2 S_y(\omega)\, d\omega \geqslant 0.$$

В последнем выражении $G(\mathrm{i}\omega)$ и $H(\mathrm{i}\omega)$ представляют собой частотные характеристики этих двух фильтров, а $S_y(\omega)$ — спектральную плотность мощности процесса $y(t)$. Заметим также, что решение $h(t)$ единственно в том смысле, что разность ошибок равна нулю только тогда, когда $G(\mathrm{i}\omega) = H(\mathrm{i}\omega)$ для всех ω, для которых $S_y(\omega) \neq 0$.

Этот результат, однако, имеет небольшую практическую ценность до тех пор, пока каким-либо образом не получено явное решение для $h(t)$ или, что эквивалентно, для $H(\mathrm{i}\omega)$. Для этого перепишем равенство (5.5) в частотной области. Делая подстановку $R(\tau) = \frac{1}{2\pi}\int_{-\infty}^{\infty} S(\omega) e^{\mathrm{i}\omega t}\, d\omega$ и меняя порядок интегрирования, находим, что

$$\sigma_e^2=\frac{1}{2\pi}\int\limits_{-\infty}^{\infty}[S_z(\omega)-S_{yz}(\omega)H(-\mathrm{i}\,\omega)-S_{zy}(\omega)H(\mathrm{i}\omega)+S_y(\omega)\,|\,H(\mathrm{i}\,\omega)|^2]\,d\,\omega=$$

$$=\frac{1}{2\pi}\int\limits_{-\infty}^{\infty}\left\{\left|\Phi(\omega)\,H(\mathrm{i}\,\omega)-\frac{S_{yz}(\omega)}{\Phi^*(\omega)}\right|^2+\left[S_z(\omega)-\frac{|\,S_{yz}(\omega)\,|^2}{S_y(\omega)}\right]\right\}d\,\omega, \qquad (5.10)$$

где $\Phi(\omega)$ — функция, удовлетворяющая соотношению $|\Phi(\omega)|^2=S_y(\omega)$, и $\Phi^*(\omega)$ — комплексно-сопряженная функция. Функции $S_z(\omega)$ и $S_y(\omega)$, как обычно, обозначают спектральные плотности мощностей процессов $z(t)$ и $y(t)$ соответственно, а $S_{zy}(\omega)$ — их взаимную спектральную плотность.

Если не требуется физическая реализуемость, то оптимальный фильтр легко найти из равенства (5.10). Так как только первый член последнего подынтегрального выражения зависит от $H(\mathrm{i}\omega)$ и так как этот член не может быть отрицательным, то среднеквадратическая ошибка минимизируется приравниванием его нулю. Таким образом,

$$H(\mathrm{i}\,\omega)=S_{yz}(\omega)/S_y(\omega) \qquad (5.11)$$

является частотной характеристикой оптимального физически нереализуемого фильтра. Получающаяся среднеквадратическая ошибка имеет вид

$$\sigma_0^2=\frac{1}{2\pi}\int\limits_{-\infty}^{\infty}\frac{S_y(\omega)\,S_z(\omega)-|\,S_{yz}(\omega)\,|^2}{S_y(\omega)}\,d\,\omega. \qquad (5.12)$$

В силу того что дополнительные ограничения на $H(\mathrm{i}\omega)$ могут лишь увеличить ошибку, $\sigma^2{}_0$, определенная равенством (5.12), часто называется *остаточной* ошибкой.

К сожалению, импульсный отклик фильтра, определяемый частотной характеристикой (5.11), не будет равен нулю для отрицательных значений t, и, следовательно, такой фильтр не будет физически реализуемым. Чтобы наложить условие физической реализуемости, удобно предположить, что спектр $S_y(\omega)$ входного процесса $y(t)$ — рациональная функция ω. Оптимизация не требует, чтобы спектр был рациональным, но рассуждения сильно упрощаются, когда рассматривается этот случай. Кроме того, спектр процесса $y(t)$ может быть в общем случае аппроксимирован сколь угодно точно рациональной функцией даже, если сам он не является рациональным.

Если спектр $S_y(\omega)$ рациональный, то его можно записать в виде

$$S_y(\omega)=a^2\,\frac{(\omega-\alpha_1)\;\ldots\;(\omega-\alpha_m)}{(\omega-\beta_1)\;\ldots\;(\omega-\beta_n)}\,. \qquad (5.13)$$

Так как $S_y(\omega)$ — спектральная плотность процесса $y(t)$, то она должна быть действительной неотрицательной симметричной функцией ω. Отсюда следует, что в приведенном выше выражении множитель a^2 должен быть действительным; любые полюса и нули с ненулевыми мнимыми частями должны появляться в виде комплексно-сопряженных пар, и все действительные полюса и нули должны иметь четную кратность.

Как следствие этих ограничений, накладываемых на спектральную плотность процесса $y(t)$, $S_y(\omega)$ можно представить в виде произведения двух выражений:

$$S_y(\omega) = a\frac{(\omega-\alpha_1)\ \ldots\ (\omega-\alpha_{m/2})}{(\omega-\beta_1)\ \ldots\ (\omega-\beta_{n/2})}\, a\frac{(\omega-\alpha_1^*)\ \ldots\ (\omega-\alpha_{m/2}^*)}{(\omega-\beta_1^*)\ \ldots\ (\omega-\beta_{n/2}^*)} \overset{\Delta}{=} \Psi(\omega)\,\Psi^*(\omega), \tag{5.14}$$

где (*) обозначена комплексно-сопряженная функция. Факторизация такова, что все полюса и нули $\Psi(\omega)$ лежат в верхней половине, а для $\Psi^*(\omega)$ — в нижней половине комплексной ω-плоскости. (В последующих выкладках удобно предположить, что $S_y(\omega)$ и, следовательно, $\Psi(\omega)$ и $\Psi^*(\omega)$ не имеют особенностей на действительной ω-оси. Если же $S_y(\omega)$ имеет такие особенности, то они должны иметь четную кратность. Поэтому они могут быть сдвинуты с оси как комплексно-сопряженные пары с помощью подстановок вида $\omega^2{}_i \to \omega^2{}_i + \varepsilon^2{}_i$. Оптимальный фильтр можно определить для этого модифицированного спектра, а требуемое решение получается теперь в пределе, когда ε_i стремится к нулю.)

Как было упомянуто, решение задачи фильтрации может быть найдено, даже если спектр $S_y(\omega)$ не является рациональным. В действительности, если

$$\int\limits_{-\infty}^{\infty} \left| \frac{\log S_y(\omega)}{1+(\omega/2\pi)^2} \right| d\omega < \infty, \tag{5.15}$$

то $S_y(\omega)$ можно еще факторизовать и получить решение. Если, с другой стороны, интеграл в ф-ле (5.15) бесконечен, то стационарный процесс $y(t)$ является *детерминированным*; будущее поведение функции может быть точно предсказано с помощью линейной операции над его прошлым.

Для последующих рассуждений удобно ввести следующее обозначение. Пусть $F(\omega)$ и $f(t)$ — пара преобразований Фурье:

$$f(t) = \int\limits_{-\infty}^{\infty} F(\omega)\, e^{i\omega t} \frac{d\omega}{2\pi}; \quad F(\omega) = \int\limits_{-\infty}^{\infty} f(t)\, e^{-i\omega t}\, dt.$$

Определим

$$f_+(t) = \begin{cases} f(t), & t \geqslant 0; \\ 0, & t < 0; \end{cases} \tag{5.16}$$

$$f_-(t) = \begin{cases} 0, & t \geqslant 0; \\ f(t), & t < 0, \end{cases} \tag{5.17}$$

так что $f(t) = f_+(t) + f_-(t)$. Теперь пусть $F_+(\omega)$ и $f_+(t)$; $F_-(\omega)$ и $f_-(t)$ — пары преобразований Фурье. Тогда $F(\omega) = F_+(\omega) + F_-(\omega)$, где преобразование первого из слагаемых является ненулевым только при $t \geqslant 0$, а преобразование второго слагаемого — только при $t<0$.

Возвращаясь к рассматриваемой задаче, найдем частотную характеристику $H(\mathrm{i}\omega)$ *физически реализуемого* фильтра, минимизирующего среднеквадратическую ошибку, задаваемую (5.10). Полагая

$$F(\omega)=\Psi(\omega)H(\mathrm{i}\,\omega)-\frac{S_{yz}(\omega)}{\Psi^*(\omega)}=F_+(\omega)+F_-(\omega), \tag{5.18}$$

можно переписать (5.10) с $\Phi(\omega)=\Psi(\omega)$ в виде

$$\sigma_e^2=\frac{1}{2\pi}\int\limits_{-\infty}^{\infty}|F(\omega)|^2 d\,\omega+\sigma_0^2=\frac{1}{2\pi}\int\limits_{-\infty}^{\infty}[\,|F_+(\omega)|^2+F_+(\omega)F_-^*(\omega)+$$

$$+F_+^*(\omega)F_-(\omega)+|\,F_-(\omega)\,|^2]\,d\,\omega+\sigma_0^2\,, \tag{5.19}$$

где $\sigma^2{}_0$ определяется равенством (5.12) и не зависит от $H(\mathrm{i}\omega)$. Но

$$\frac{1}{2\pi}\int\limits_{-\infty}^{\infty}F_+(\omega)F_-^*(\omega)\,d\,\omega=\frac{1}{2\pi}\int\limits_{-\infty}^{\infty}F_-^*(\omega)\int\limits_{-\infty}^{\infty}f_+(t)\,\mathrm{e}^{-\mathrm{i}\omega t}\,dt\,d\,\omega=$$

$$=\int\limits_{-\infty}^{\infty}f_+(t)\,\frac{1}{2\pi}\int\limits_{-\infty}^{\infty}F_-^*(\omega)\,\mathrm{e}^{-\mathrm{i}\omega t}\,d\,\omega\,dt=\int\limits_{-\infty}^{\infty}f_+(t)f_-^*(t)dt=0. \tag{5.20}$$

То же справедливо для интеграла $\frac{1}{2\pi}\int\limits_{-\infty}^{\infty}F_+^*(\omega)F_-(\omega)\,d\,\omega$. Далее

$$F_-(\omega)=[\Psi(\omega)H(\mathrm{i}\,\omega)]_- - \left[\frac{S_{yz}(\omega)}{\Psi^*(\omega)}\right]_- = -\left[\frac{S_{yz}(\omega)}{\Psi^*(\omega)}\right]_- . \tag{5.21}$$

Выражение (5.21) не зависит от $H(\mathrm{i}\omega)$. Это следует из того, что

$$\frac{1}{2\pi}\int\limits_{-\infty}^{\infty}\Psi(\omega)\;H(\mathrm{i}\,\omega)\,\mathrm{e}^{\mathrm{i}\,\omega t}\,d\,\omega=\int\limits_{-\infty}^{\infty}\Phi(\eta)\,h(t-\eta)\,d\,\eta, \tag{5.22}$$

где функции $\Phi(t)$ (преобразование Фурье $\Psi(\omega)$) и $h(t)$ равны нулю для всех $t<0$ 1). Таким образом, свертка в (5.22) равна нулю для всех $t<0$; $[\Psi(\omega)H(\mathrm{i}\omega)]_-=0$ и равенство (5.21) справедливо. Единственный член в ф-ле (5.19), зависящий от $H(\mathrm{i}\omega)$, имеет вид

$$F_+(\omega)=[\Psi(\omega)H(\mathrm{i}\,\omega)]_+ - \left[\frac{S_{yz}(\omega)}{\Psi^*(\omega)}\right]_+ = \Psi(\omega)H(\mathrm{i}\omega)-\left[\frac{S_{yz}(\omega)}{\Psi^*(\omega)}\right]_+ , \tag{5.23}$$

что следует непосредственно из (5.22) (т. е. преобразование Фурье

---

1) Следует помнить, что $f(t)$ не равна нулю при $t>0$ только тогда, когда ее (рациональное) преобразование $F(\omega)$ имеет полюсы в верхней ω-полуплоскости (левой s-полуплоскости, где $s=\mathrm{i}\omega$) и не равна нулю при $t<0$ только тогда, когда $F(\omega)$ имеет полюсы в нижней ω-полуплоскости. (*Прим. авт.*).

функции $\Psi(\omega)H(i\omega)$ отлично от нуля лишь при $t\geqslant 0$). Частотная характеристика оптимального физически реализуемого фильтра теперь определяется приравниванием этого члена нулю:

$$H(i\,\omega)=\frac{1}{\Psi(\omega)}\left[\frac{S_{yz}(\omega)}{\Psi^*(\omega)}\right]_+ . \tag{5.24}$$

Любой другой физически реализуемый фильтр необходимо приводит к бо́льшей среднеквадратической ошибке.

Если выражение, стоящее в квадратных скобках в ф-ле (5.24), рационально, то $H(i\omega)$ можно определить довольно легко, производя разложение этого выражения на простейшие дроби и оставляя только полюса, лежащие в верхней ω-полуплоскости. Если оно нерационально, то вначале можно найти его преобразование Фурье и затем оставить лишь ту часть этого преобразования, которая соответствует положительному времени. В результате получим

$$H(i\,\omega)=\frac{1}{\Psi(\omega)}\int\limits_0^{\infty} e^{-i\omega t}\left[\frac{1}{2\pi}\int\limits_{-\infty}^{\infty} e^{i\,\omega' t}\,\frac{S_{yz}(\omega')}{\Psi^*(\omega')}\,d\,\omega'\right]dt. \tag{5.25}$$

До сих пор мало было сказано о желаемом сигнале $z(t)$. Предполагалось лишь, что $S_z(\omega)$ и $S_{yz}(\omega)$ определены. В самом обычном случае $y(t)=x(t)+n(t)$, где сигнал $x(t)$ и шум $n(t)$ — ортогональные случайные процессы ($R_{xn}(\tau)=0$), а $z(t)=x(t+t_0)$ для некоторого постоянного t_0. (Если $t_0=-\infty$, что соответствует бесконечному времени задержки, то оптимальный фильтр опять физически нереализуем [см. ф-лу (5.11)]; считается, что сигнал известен на всем интервале $-\infty<t<+\infty$.) В этих условиях

$$S_y(\omega)=S_x(\omega)+S_n(\omega) \text{ и } S_{yz}(\omega)=S_x(\omega)\,e^{i\omega t_0} .$$

Если $t_0>0$, то результирующий фильтр называется *предсказывающим* фильтром.

Фильтр, представляющий наибольший интерес, называется *сглаживающим* фильтром и соответствует случаю $z(t)=x(t)$ и $y(t)=x(t)+n(t)$. Равенство (5.14) может быть несколько упрощено, когда $t_0=0$, а спектры (ортогональных) сигнала и шума рациональны. Для этого случая

$$H(i\,\omega)=\frac{1}{\Psi(\omega)}\left[\frac{S_x(\omega)}{\Psi^*(\omega)}\right]_+=\frac{1}{\Psi(\omega)}\left[\frac{\Psi(\omega)\Psi^*(\omega)-S_n(\omega)}{\Psi^*(\omega)}\right]_+=$$

$$=1-\frac{1}{\Psi(\omega)}\left[\frac{S_n(\omega)}{\Psi^*(\omega)}\right]_+ . \tag{5.26}$$

Если, кроме того, шум белый, $S_n(\omega)=N_0/2$ и спектральная плотность сигнала стремится к нулю для больших ω, то это выражение можно упростить еще больше. Так как

$$\lim_{\omega\to\infty}\Psi(\omega)\Psi^*(\omega)=\lim_{\omega\to\infty}\left[S_x(\omega)+\frac{N_0}{2}\right]=\frac{N_0}{2} ,$$

то $\lim\limits_{\omega\to\infty}\Psi(\omega)=\lim\limits_{\omega\to\infty}\Psi^*(\omega)=(N_0/2)^{1/2}$ и выражение $S_n(\omega)/\Psi^*(\omega)$ имеет ненулевой вычет при $\omega=\infty$. Однако

$$\left[\frac{S_n(\omega)}{\Psi^*(\omega)}\right]_+=\left[\left(\frac{N_0}{2}\right)^{1/2}-\left(\frac{N_0}{2}\right)^{1/2}\frac{\Psi^*(\omega)-\left(\frac{N_0}{2}\right)^{1/2}}{\Psi^*(\omega)}\right]_+=$$

$$=\left(\frac{N_0}{2}\right)^{1/2}-\left(\frac{N_0}{2}\right)^{1/2}\left[\frac{\Psi^*(\omega)-\left(\frac{N_0}{2}\right)^{1/2}}{\Psi^*(\omega)}\right]_+, \tag{5.27}$$

а этот последний член имеет нулевой вычет при $\omega=\infty$. Следовательно, его разложение на простейшие дроби содержит только дроби вида $K/(\omega+\alpha)^k$ (где k — положительное целое число) и, так как все нули $\Psi^*(\omega)$ лежат в нижней полуплоскости, то

$$\left[\frac{\Psi^*(\omega)-(N_0/2)^{1/2}}{\Psi^*(\omega)}\right]_+=0.$$

Таким образом, если шум является белым и ортогональным сигналу и если спектральная плотность сигнала $S_x(\omega)$ — рациональная функция ω, а $\lim\limits_{\omega\to\infty}S_x(\omega)=0$, то

$$H(\mathrm{i}\,\omega)=1-\frac{1}{\Psi(\omega)}\left[\frac{S_n(\omega)}{\Psi^*(\omega)}\right]_+=1-\frac{\left(\frac{N_0}{2}\right)^{1/2}}{\Psi(\omega)}. \tag{5.28}$$

Среднеквадратическая ошибка, соответствующая оптимальному фильтру, задается равенством (5.28). Представляют интерес также эквивалентные выражения в частотной области

$$\sigma_e^2=\frac{1}{2\pi}\int\limits_{-\infty}^{\infty}[S_z(\omega)-S_y(\omega)\mid H(\mathrm{i}\,\omega)|^2]\,d\,\omega=$$

$$=\frac{1}{2\pi}\int\limits_{-\infty}^{\infty}[S_z(\omega)-S_{yz}(\omega)\,H(-\mathrm{i}\,\omega)]\,d\,\omega. \tag{5.29}$$

Когда $z(t)=x(t)$; $y(t)=x(t)+n(t)$ и $x(t)$ и $n(t)$ — ортогональные процессы, эти равенства принимают вид

$$\sigma_e^2=\frac{1}{2\pi}\int\limits_{-\infty}^{\infty}\{S_x(\omega)[1-|H(\mathrm{i}\,\omega)|^2]-S_n(\omega)\,|H(\mathrm{i}\,\omega)|^2\}\,d\,\omega=$$

$$=\frac{1}{2\pi}\int\limits_{-\infty}^{\infty}S_x(\omega)[1-H(\mathrm{i}\,\omega)]\,d\,\omega. \tag{5.30}$$

Это выражение особенно удобно, если использовать либо равенство (5.26), либо (5.28). В последнем случае

$$\sigma_e^2=\left(\frac{N_0}{2}\right)^{1/2}\int\limits_{-\infty}^{\infty}\frac{S_x(\omega)}{\Psi(\omega)}\,\frac{d\,\omega}{2\pi}. \tag{5.31}$$

Еще одно полезное выражение для среднеквадратической ошибки при тех же самых условиях следует из равенства (5.10):

$$\sigma_e^2 = \frac{1}{2\pi}\int\limits_{-\infty}^{\infty}[S_x(\omega)\,|\,1 - H(\mathrm{i}\,\omega)\,|^2 + S_n(\omega)\,|\,H(\mathrm{i}\,\omega)\,|^2]\,d\,\omega. \tag{5.32}$$

Это равенство, в отличие от предыдущих выражений для ошибки, справедливо даже тогда, когда $H(\mathrm{i}\omega)$ является характеристикой неоптимального фильтра.

5.3. Пересмотр теории согласованных фильтров

В гл. 3 и 4 было установлено, что все без исключения формулы оценок параметров и приемники содержат *согласованные фильтры,* т. е. фильтры с импульсными откликами вида

$$h(t) = f(t_0 - t), \tag{5.33}$$

где функция $f(t)$ $(0<t<t_0)$ связана с ожидаемым сигналом. В этом параграфе покажем интересную взаимосвязь между оптимальными в смысле среднеквадратической ошибки фильтрами и согласованными фильтрами. С этой целью поставим другую задачу, которая также имеет в качестве решения согласованный фильтр вида (5.33), но решается методами, развитыми в предыдущем параграфе. Задача состоит в следующем. Принимаемый сигнал имеет вид $y(t)=f(t)+n(t)$, где $f(t)$ — известная функция времени, а $n(t)$ — шум, стационарный в широком смысле случайный процесс. Сигнал следует пропустить через линейный фильтр с импульсным откликом $h(t)$. Обозначим через $g(t)$ выход этого фильтра, который наблюдался бы в случае отсутствия шума, и через $\sigma^2{}_n$ — среднеквадратическое значение шумовой компоненты выходного сигнала фильтра. Задача состоит в отыскании фильтра с импульсным откликом $h(t)$, который максимизирует отношение

$$g^2(t_0)/\sigma_n^2\,, \tag{5.34}$$

где t_0 — некоторый фиксированный момент времени[1]. Так как представляет интерес отношение сигнал/шум, а не уровень сигнала сам по себе, эта максимизация может быть выполнена, если потребовать, чтобы составляющая сигнала на выходе принимала некоторое фиксированное значение в момент времени $t=t_0$, и найти фильтр, который минимизирует среднеквадратический уровень шума. В соответствии с этим, так как

$$g(t_0) = \int\limits_{-\infty}^{\infty} h(t_0 - t)\,f(t)\,dt = \frac{1}{2\pi}\int\limits_{-\infty}^{\infty} \mathrm{e}^{\mathrm{i}\omega t_0}\,H(\mathrm{i}\,\omega)\,F(\mathrm{i}\,\omega)\,d\,\omega,$$

---

[1] Так как $f(t)$ — известная функция времени, то процесс $y(t)$ не является стационарным. Следовательно, в противоположность фильтрам, рассмотренным в предыдущих параграфах, оптимальный фильтр, рассматриваемый здесь в общем случае, будет зависеть от заданного момента времени t_0. *(Прим. авт.).*

где $F(\mathrm{i}\omega)=\int\limits_{-\infty}^{\infty} f(t)\mathrm{e}^{-\mathrm{i}\omega t}dt$, требуется найти частотную характеристику $H(\mathrm{i}\omega)$, которая минимизирует выражение

$$\sigma_n^2+\lambda g(t_0)=\frac{1}{2\pi}\int\limits_{-\infty}^{\infty}\Big\{|H(\mathrm{i}\,\omega)|^2 S_n(\omega)+\frac{\lambda}{2}\mathrm{e}^{\mathrm{i}\omega t_0}H(\mathrm{i}\,\omega)F(\mathrm{i}\,\omega)+$$

$$+\frac{\lambda}{2}\mathrm{e}^{-\mathrm{i}\,\omega t_0}H(-\mathrm{i}\,\omega)F(-\mathrm{i}\,\omega)\Big\}d\omega. \qquad (5.35)$$

Это выражение совпадает с (5.10) после подстановки величин $S_n(\omega)$; $-(\lambda/2)\mathrm{e}^{-\mathrm{i}\omega t_0}F(-\mathrm{i}\omega)$ и 0 вместо $S_y(\omega)$; $S_{yz}(\omega)$ и $S_z(\omega)$ соответственно. Единственным ограничением, наложенным на эти выражения при выводе ф-лы (5.25) для оптимального физически реализуемого фильтра, было то, что $S_y(\omega)$ (или в рассматриваемом случае $S_n(\omega)$) факторизуемо. Таким образом, если $S_n(\omega)=\Psi(\omega)\Psi^*(\omega)$ и все особенности $\Psi(\omega)$ лежат в верхней ω-полуплоскости, то оптимальный физически реализуемый фильтр в рассматриваемой задаче имеет частотную характеристику

$$H(\mathrm{i}\,\omega)=\frac{k}{\Psi(\omega)}\int\limits_{0}^{\infty}\mathrm{e}^{-\mathrm{i}\omega t}\frac{1}{2\pi}\int\limits_{-\infty}^{\infty}\frac{\mathrm{e}^{\mathrm{i}\omega'(t-t_0)}F(-\mathrm{i}\,\omega')}{\Psi^*(\omega')}d\omega'\,dt, \qquad (5.36)$$

где $k=-\lambda/2$ — постоянный коэффициент усиления, который не влияет на отношение сигнал/шум. Если шум является белым, $S_n(\omega)=N_0/2$, то

$$\frac{1}{2\pi}\int\limits_{-\infty}^{\infty}\frac{\mathrm{e}^{\mathrm{i}\omega'(t-t_0)}F(-\mathrm{i}\omega')}{(N_0/2)^{1/2}}d\omega'=\frac{1}{(N_0/2)^{1/2}}f(t_0-t)$$

и $$H(\mathrm{i}\,\omega)=k_1\int\limits_{0}^{\infty}f(t_0-t)\,\mathrm{e}^{-\mathrm{i}\omega t}dt, \qquad (5.37)$$

где $k_1=2k/N_0$ — произвольная постоянная. Таким образом, положив $k_1=1$, получаем

$$h(t)=\begin{cases} f(t_0-t), & t>0;\\ 0 & t<0.\end{cases} \qquad (5.38)$$

Если $f(t)$ — тождественный нуль при $t>t_0$, то полученное выражение в действительности представляет собой импульсный отклик согласованного фильтра, определенного в гл. 3.

5.4. Формулы оценок при отслеживании фазы

Предположим, что $Ax(t)$ — известный периодический сигнал с периодом T, имеет неизвестную задержку по времени τ секунд и принимается на фоне аддитивного гауссовского белого шума $n(t)$ (с односторонней спектральной плотностью N_0). Пусть требуется оценить τ по принятому сигналу $y_l(t)=Ax(t+\tau)+n(t)$; $lT<t<(l+1)T$. (Так как τ можно оценить только с точностью до периода T, то оно может быть либо отрицательным, либо положительным.) Оценка максимального правдоподобия величины τ в этих условиях является решением уравнения (см. § 3.4)

$$\frac{\partial}{\partial\hat{\tau}}\log_e p(y_l(t)\,|\,\hat{\tau})=\frac{\partial}{\partial\hat{\tau}}\left\{\frac{1}{N_0}\int\limits_{lT}^{(l+1)T}[2Ay_l(t)\,x(t+\hat{\tau})-A^2x^2(t+\hat{\tau})]\right\}dt=$$

$$=\frac{2A}{N_0}\int\limits_{lT}^{(l+1)T}y_l\,(t)\frac{\partial x\,(t+\hat{\tau})}{\partial\hat{\tau}}\,dt=0. \qquad (5.39)$$

В некоторых случаях, когда, например $x(t)$ — синусоида, ур-ние (5.39) приводит к решению в явном виде для оптимальной оценки $\hat{\tau}$ задержки τ (см. § 3.7). В более общем случае это не так. В любом случае задача, которая здесь рассматривается, в некотором отношении отличается от рассмотренных в гл. 3. Здесь предполагается, что τ, в отличие от случая, когда она принимает независимые значения на каждом последовательном интервале в T секунд, является непрерывной функцией времени, примерно постоянной на любом заданном интервале, но медленно изменяющейся от одного интервала к другому.

В силу того что τ предполагается почти постоянной на любом T-секундном интервале, можно было бы произвести независимые оценки ее по максимуму правдоподобия на каждом из этих интервалов, используя формулу оценки (5.39). Но так как τ — медленно меняющаяся функция времени, то ее значения на последовательных интервалах будут сильно коррелированы. Игнорирование этой корреляции приводит к потере полезной информации. Если было бы возможно точно описать условную плотность распределения $p(\tau_l\,|\,\hat{\tau}_{l-1},\ \hat{\tau}_{l-2},\ldots)$ величины τ на интервале $lT<t<(l+1)T$ при условии, что заданы оценки величин τ на предыдущих интервалах, то формула оценки по максимуму апостериорной вероятности, в принципе, могла бы быть найдена.

Часто более практичным методом, позволяющим получить почти тот же самый результат, является метод, использующий тот факт, что при соблюдении определенных условий регулярности

$$E\left[\left(\frac{\partial\log_e p\,[y_l\,(t)\ |\ \hat{\tau}]}{\partial\hat{\tau}}\right)_{\hat{\tau}=\tau}\middle|\,\tau\right]=0; \qquad (5.40)$$

$$E\left[\left(\frac{\partial^2\log_e p\,[y_l\,(t)\ |\ \hat{\tau}]}{\partial^2\hat{\tau}}\right)_{\hat{\tau}=\tau}\middle|\,\tau\right]=-E\left[\left(\frac{\partial\log_e p\,(y_l\,(t)\ |\ \hat{\tau})}{\partial\hat{\tau}}\right)^2_{\hat{\tau}=\tau}\middle|\,\tau\right]. \qquad (5.41)$$

Таким образом, математическое ожидание величины интеграла

$$e_l = \int_{lT}^{(l+1)T} y_l(t)\,\frac{\partial x(t+\hat{\tau})}{\partial \hat{\tau}}\,dt \tag{5.42}$$

является монотонно убывающей функцией τ в окрестности $\hat{\tau}\approx\tau$, положительной при $\hat{\tau}<\tau$ и отрицательной при $\hat{\tau}>\tau$. Предположим поэтому, что величины e_l используют для управления изменением фазы $\hat{\tau}$ сигнала местного генератора, заставляя $\hat{\tau}$ уменьшаться, когда величина (e_l) отрицательна, и увеличиваться, когда она положительна. Вообще говоря, в случае, если $\hat{\tau}=\tau$ — единственное значение $\hat{\tau}$, для которого выполняются соотношения (5.40) и (5.41), то $\hat{\tau}$ будет сходиться к τ и отслеживать τ. В действительности, чтобы использовать факт медленного изменения $\hat{\tau}$ во времени, $\hat{\tau}$ должно управляться взвешенным средним прошлых показаний индикатора знака ошибки $\tau-\hat{\tau}$, т. е. величиной вида $\varepsilon_{l+1}\triangleq\sum\limits_{i=-\infty}^{l}\alpha_{l-i}e_i$, а не только одной величиной e_l.

Функциональная схема устройства, выполняющего описанные операции, изображена на рис. 5.1. Если $h(0)=0$ и

$$h_\alpha(t)=\alpha_i;\quad iT<t<(i+1)T, \tag{5.43}$$

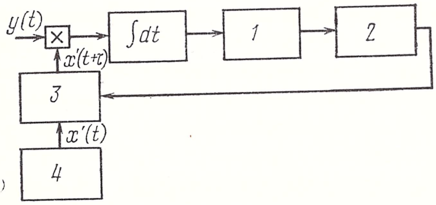


Рис. 5.1. Устройство отслеживания фазы:
1 — устройство, производящее выборки; *2* — устройство, усредняющее с весом; *3* — фазовращатель; *4* — генератор сигнала

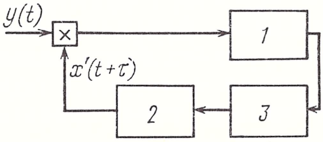


Рис. 5.2. Структурная схема системы ФАПЧ:
1 — фильтр ФАПЧ; *2* — генератор сигнала; *3* — ГУН

то входной сигнал фазовращателя на интервале $(l+1)T<t<(l+2)T$ можно представить в виде

$$\varepsilon_{l+1}=\sum_{i=-\infty}^{l}\alpha_{l-i}\,e_i\triangleq\varepsilon((l+1)T), \tag{5.44}$$

где $\varepsilon(t)\triangleq\int\limits_{-\infty}^{t}y(\eta)\,x'(\eta+\hat{\tau})\,h_\alpha(t-\eta)\,d\eta$. Более того, если τ, как предполагалось, относительно постоянна на любом интервале в T секунд, то разность $\alpha_i-\alpha_{i-1}$ должна быть малой при всех i. Следовательно, $h_\alpha(t)$ может быть точно аппроксимирована непрерывной (и даже дифференцируемой) функцией времени, скажем $h'_\alpha(t)$, и входы фазосдвигающего устройства ε_l могут быть заменены на входной сигнал $\varepsilon(t)$ без какого-либо существенного влияния на характеристики устройства. Наконец, заметим, что вместо того, чтобы устанавливать связь $\hat{\tau}$ непосредственно с функцией $\varepsilon(t)$, можно, что эквивалентно, установить связь между скоростью изменения $\hat{\tau}$ и производной этой функции:

$$\varepsilon'(t) = \int_{-\infty}^{t} y(\eta)\, x'(\eta + \hat{\tau})\, h'_\alpha(t - \eta)\, d\eta. \qquad (5.45)$$

Рассмотрим теперь устройство, представленное функциональной схемой на рис. 5.2. Генератор, управляемый напряжением (ГУН), генерирует колебания, частота которых в идеале пропорциональна напряжению на его входе. Выход ГУН используется для синхронизации генератора сигнала, вырабатывающего местный сигнал $x'(t+\hat{\tau})$, и тем самым регулирует скорость изменения $\hat{\tau}$. Принимая во внимание результаты предыдущего абзаца, можно, следовательно, заключить, что если импульсный отклик фильтра ФАПЧ $h(t)=h'_\alpha(t)$, то устройства на рис. 5.1 и 5.2 функционально эквивалентны. Последнее устройство известно под названием *системы фазовой автоподстройки частоты* (ФАПЧ) и наиболее часто используется на практике.

Система ФАПЧ тогда является, по существу, устройством с обратной связью, предназначенным для решения уравнения правдоподобия (5.39). Еще не определенный точно фильтр ФАПЧ необходим потому, что фаза принимаемого сигнала τ изменяется со временем, поэтому при оценке текущей фазы прошлое, вообще говоря, не должно использоваться с одинаковыми весами. Возникает задача определения оптимального фильтра ФАПЧ, как функции статистик процесса $\tau(t)$. Однако, прежде чем решить эту задачу, необходимо разработать линейную модель системы ФАПЧ. Это сделано в следующем параграфе. Для того чтобы избежать усложнения изложения, предположим, что $x(t)$ — синусоида. Полученные результаты обобщаются в § 5.8 также на несинусоидальные функции.

Полезно вновь подчеркнуть, что одно из фундаментальных различий между методом сглаживающего фильтра и методом согласованного фильтра в задаче оценивания состоит в количестве априорных знаний о сигнале. Согласованный фильтр требует полного описания ожидаемого сигнала за исключением, быть может, неизвестного, но постоянного параметра или параметров; сглаживающий фильтр требует лишь знания его статистических характеристик второго порядка. В рассматриваемом случае оба подхода, как окажется, применимы к одной и той же задаче. Согласованный фильтр может быть использован в силу того, что функциональный вид ожидаемого сигнала известен, исключая неизвестный параметр; однако теперь этот параметр является случайным процессом, а не случайной величиной. Сглаживающий фильтр потребуется, следовательно, для наиболее точной, по возможности, непрерывной оценки этого меняющегося по времени параметра.

5.5. Линейная модель

Функциональная схема системы ФАПЧ для отслеживания фазы синусоидального сигнала изображена на рис. 5.3. Так как выход ГУН сам является синусоидой, генератор сигнала на рис. 5.2 может быть заменен фазовращателем с поворотом фазы на 90° или даже вовсе опущен. (Поворот на 90° необходим, если выход ГУН должен служить копией принятого сигнала.) Точный анализ ошибки отслеживания, связанной с этим устройством, является сложным. Из-за нелинейности дифференциального уравнения, связывающего выход и вход устройства, оно может быть решено точно лишь в некоторых частных случаях. Для того чтобы получить пригодные для работы результаты, касающиеся характеристики системы, а также определить вид оптимального фильтра ФАПЧ, необходимо сделать приближение, которое приведет к линеаризации дифференциального уравнения системы. Справедливость этого линейного приближения зависит от того, насколько велико отношение сигнал/шум и, следовательно, насколько мала ошибка отслеживания. В большинстве применений, которые нас будут интересовать, это условие будет обязательно выполнено.

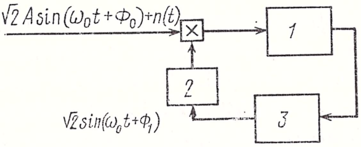

$\sqrt{2}A\sin(\omega_0 t+\Phi_0)+n(t)$
×
1
2
3
$\sqrt{2}\sin(\omega_0 t+\Phi_1)$

Рис. 5.3. Структурная схема синусоидальной ФАПЧ:

1 — фильтр ФАПЧ; *2* — поворот фазы на 90°; *3* — ГУН

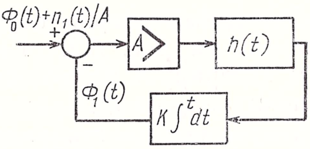


Рис. 5.4. Функциональная схема линейной модели системы ФАПЧ

Если принимаемый сигнал имеет вид $y(t)=\sqrt{A}\sin[\omega_0 t+\Phi_0(t)]+n(t)$ и если выход сдвинутого по фазе ГУН равен $\sqrt{2}\cos[\omega_0 t+\Phi_1(t)]$, то при выполнении указанного выше условия $\Phi_0(t)\approx\Phi_1(t)$. Низкочастотная компонента произведения этих функций $A\sin[\Phi_0(t)-\Phi_1(t)]\approx A[\Phi_0(t)-\Phi_1(t)]$ поэтому является приближенно линейной функцией разности фаз. Кроме того, компонентой удвоенной частоты этого произведения можно полностью пренебречь вследствие того, что система ФАПЧ, по существу, эквивалентна устройству на рис. 5.1 и, следовательно, реагирует лишь на интеграл этого произведения по полному периоду. Скорость изменения фазы (т. е. частота) выхода ГУН теперь (приближенно) пропорциональна профильтрованной и искаженной шумом ошибке отслеживания:

$$\Phi_0(t)-\Phi_1(t)\triangleq\Phi_e(t). \tag{5.46}$$

Следовательно, до тех пор, пока ошибка отслеживания является малой, система ФАПЧ может быть представлена так, как показано на рис. 5.4.

Для анализа этой модели нужно определить статистические характеристики входного шума $n_1(t)\triangleq\sqrt{2}\cos[\omega_0 t+\Phi_1(t)]n(t)\triangleq\alpha(t)n(t)$. Исследование, казалось бы, сильно усложняется зависимостью между этим шумом и фазой на выходе ГУН. Но эта фаза зависит не от самого процесса $n(t)$, а от интеграла от профильтрованного произведения $n(t)\alpha(t)$. Если ширина полосы шума равна B_n, то величины $n(t)$ и $n(t-\tau)$, по существу, независимы при любых $\tau>k/B_n$, где k — обычно малое число. Так как фаза $\Phi_0(t)$ по предположению медленно меняется по сравнению с периодом сигнала $2\pi/\omega_0$, то оптимальная оценка $\Phi_1(t)$ фазы будет зависеть от значений входного сигнала в последние $2\pi K/\omega_0$ секунд, где $K\gg 1$. В соответствии с этим, если $\omega_0/2\pi K\triangleq B_l\ll B_n$ (а выполнение этого неравенства, конечно, необходимо, чтобы назвать шум «белым»), то шум, принятый в последние k/B_n секунд, будет пренебрежимо мало влиять на $\Phi_1(t)$. Поэтому $\Phi_1(t)$ и, как следствие, $\alpha(t)$ не будут, по существу, зависеть от $n(t)$ и

$$E\{n_1(t)\}\approx E\{n(t)\}E\{\alpha(t)\}=0, \tag{5.47}$$

в то время как

$$E\{n_1(t_1)n_1(t_2)\}\approx\begin{cases}E\{n(t_1)\alpha(t_1)\alpha(t_2)\}E\{n(t_2)\}=0, & t_2>t_1;\\ E\{n^2(t_1)\}E\{\alpha^2(t_1)\}, & t_2=t_1.\end{cases} \tag{5.48}$$

Но если входной шум—белый (т. е. $B_n\gg B_l$), то $E\{n(t)n(t+\tau)\}\approx\approx\frac{N_0}{2}\delta(\tau)$, так что

$$E\{n_1(t)n_1(t+\tau)\}\approx\frac{N_0}{2}E\{\alpha^2(t)\}\delta(\tau). \tag{5.49}$$

Если фаза $\Phi_0(t)$ распределена равномерно, что предполагается, и если ошибка в фазе не зависит от $\Phi_0(t)$, что, очевидно, имеет место в системе ФАПЧ, то величина $\Phi_1(t)$ также равномерно распределена на интервале $(0, 2\pi)$. Следовательно, так как $\alpha(t)=\sqrt{2}\cos[\omega_0 t+\Phi_1(t)]$, то $E[\alpha^2(t)]=1$. Поэтому шум на входе линейной модели системы ФАПЧ, по существу, является белым и стационарным в широком смысле.

Спектр входного шума $S_{n1}(\omega)$ только что был определен. Так как при отыскании оптимального фильтра необходимо также знание взаимной спектральной плотности $S_{n1}\Phi_0(\omega)$, то ее также следует изучить. Но так как $n(t_1)$, по существу, не зависит от $\alpha(t_1)$ и совершенно не зависит от фазы сигнала $\Phi_0(t_2)$ при любом t_2, то

$$E\{n_1(t_1)\Phi_0(t_2)\} \approx E\{\alpha(t_1)\Phi_0(t_2)\}E\{n(t_1)\} = 0 \qquad (5.50)$$

и спектральная плотность $S_{n1}\Phi_0(\omega)$ пренебрежимо мала.

Наконец, в силу того, что интересна не только дисперсия, но также и распределение фазовой ошибки $\Phi_e(t)=\Phi_0(t)-\Phi_1(t)$, полезно дать полное статистическое описание процесса $n_1(t)=n(t)\alpha(t)$, представляющего собой шум на входе. Для этого удобно предположить на некоторое время, что перед системой ФАПЧ находится полосовой фильтр с полосой $B\leqslant 2f_0=2\omega_0/2\pi$, симметрично расположенной относительно частоты f_0. Дисперсия шума $\sigma^2{}_n$ тогда равна N_0B. Пусть $n_f(f)$ обозначает, что этот шум профильтрован и

$$n_f(t)=n_a(t)\cos\omega_0 t - n_b(t)\sin\omega_0 t. \qquad (5.51)$$

Если $n(t)$ — гауссовский процесс с нулевым средним, то $n_a(t)$ и $n_b(t)$ — взаимно независимые гауссовские процессы, имеющие средние, равные нулю, и дисперсии, равные дисперсии $n_f(t)$. Так как $\alpha(t)=\sqrt{2}\cos[\omega_0 t+\Phi_1(t)]$, то низкочастотные компоненты произведения $n_f(t)\alpha(t)$ могут быть записаны в виде

$$n_f(t)\alpha(t)]_{lf} = \frac{1}{\sqrt{2}}\{n_\alpha(t)\cos\Phi_1(t)+n_b(t)\sin\Phi_1(t)\}. \qquad (5.52)$$

Положим теперь

$$\sqrt{2}\,[n_f(t)\alpha(t)]_{lf}=n'(t)=\{n_a(t)\cos\Phi_1(t)+n_b(t)\sin\Phi_1(t)\} \qquad (5.53)$$

и $n''(t)=\{n_a(t)\sin\Phi_1(t)-n_b(t)\cos\Phi_1(t)\}$ и рассмотрим совместную плотность распределения случайных величин n', n'', Φ_1 в какой-либо фиксированный момент времени. Якобиан преобразования перехода от n_a, n_b и Φ_1, к n', n'' и Φ_1 равен единице. Более того,

$$p(n_a, n_b, \Phi_1)=\frac{1}{2\pi\sigma_n^2}\,e^{-(n_a^2+n_b^2)/2\sigma_n^2}\,p(\Phi_1).$$

Последнее следует из того, что n_a и n_b — независимые гауссовские величины, а (как уже было показано) $n_f(t)$ и, следовательно, $n_a(t)$ и $n_b(t)$, по существу, не зависят от $\Phi(t)$. Но $n^2{}_a+n^2{}_b=(n')^2+(n'')^2$ и поэтому

$$p(n', n'', \Phi_1)=\frac{1}{2\pi\sigma_n^2}\,e^{-[(n')^2+(n'')^2]/2\sigma_n^2}\,p(\Phi_1).$$

Наконец,

$$p(n')=\int\limits_{-\infty}^{\infty}\int\limits_{0}^{2\pi}p(n', n'', \Phi_1)\,d\Phi_1\,dn''=\frac{1}{\sqrt{2\pi}\,\sigma_n}\,e^{-(n')^2/2\sigma_n^2}, \qquad (5.54)$$

и одномерное распределение шума на входе фильтра ФАПЧ $[n_f(t)x(t)]_{lf}=(1/\sqrt{2})n'(t)$ является гауссовским с нулевым средним и дисперсией $1/2\sigma^2_n$. Так как ширина полосы низкочастотной компоненты вдвое меньше, чем ширина полосы фильтра, то двусторонняя спектральная плотность этой компоненты равна $(1/2\sigma^2_n)/(1/2B)=N_0/2$, т. е. та же, что и у процесса $n(t)$.

Хотя в предыдущих рассуждениях было удобно рассматривать полосовой фильтр с шириной полосы $B\leqslant 2f_0$, стоящий перед системой ФАПЧ, наличие фильтра в действительности несущественно для выводов. После умножения на $\alpha(t)$ любая компонента шума вне диапазона частот $0<t<2f_0$ будет расположена далеко за пределами полосы пропускания системы ФАПЧ. Таким образом, B может быть произвольно большой, не влияя на выход цепи, и фильтр, фактически, можно полностью устранить. В соответствии с этим при рассмотрении системы ФАПЧ, процесс $[n_1(t)]_{lf}$ можно считать белым гауссовским случайным процессом со спектральной плотностью $N_0/2$. Снова высокочастотные компоненты процесса $n_1(t)$ не будут влиять на характеристики системы ФАПЧ и могут не учитываться.

5.6. Оптимизация фильтра в системе ФАПЧ

Существует несколько подходов к оптимизации системы ФАПЧ, зависящих от предположений относительно сигнала. В задаче всегда следует учитывать случайные расхождения из-за нестабильностей генератора между фазой на выходе ГУН и фазой принятого сигнала даже в отсутствие шума. Хотя в эти случайные флуктуации вносят вклад оба генератора, в общем случае удобно рассматривать ГУН как идеальный генератор, а генератор передатчика — как единственный источник этих изменений. Для большинства случаев действительный источник является несущественным, так как интересна лишь разность фаз. Если спектр этих флуктуаций фазы известен или если его можно найти приближенно, то фильтр в системе ФАПЧ можно легко оптимизировать так, чтобы минимизировать среднеквадратическую разность фаз.

Используя преобразования Лапласа $\theta_i(s)=\int\limits_0^\infty \Phi_i(t)\,\mathrm{e}^{-st}dt$, $i=0,1$ и $H(s)=\int\limits_0^\infty h(t)\mathrm{e}^{-st}dt$, где $s=\alpha+\mathrm{i}\omega$, $\alpha\geqslant 0$, получаем в отсутствие шума [ср. с рис. 5.4; $\Phi_1(t)$, $\Phi_2(t)$ и $h(t)$ те же, что и определенные на рисунке], что

$$\theta_1(s)=Y(s)\,\theta_0(s), \tag{5.55}$$

где $Y(s)$ — частотная характеристика системы ФАПЧ

$$Y(s)=\frac{AKH(s)}{s+AKH(s)} \tag{5.56}$$

(Здесь K обозначает усиление ГУН).

Это соотношение иллюстрируется рис. 5.5. Для того чтобы определить частотную характеристику оптимального фильтра $H(s)$, достаточно найти оптимальную частотную характеристику $Y(s)$ и затем выразить $H(s)$:

$$H(s) = \frac{sY(s)}{AK[1 - Y(s)]}. \tag{5.57}$$

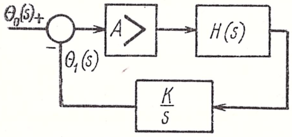


Рис. 5.5. Функциональная схема линейной модели в частотном представлении

Так как цепь, пригодная для каких-либо применений, должна быть устойчивой, то $Y(s)$ должна быть частотной характеристикой устойчивого фильтра (ср. с § 5.2). Таким образом, преобразование Фурье $Y(i\omega)$ импульсного отклика этого фильтра также существует, и процедура оптимизации, развитая в § 5.2, прямо применима здесь. Оптимальный фильтр ФАПЧ $H(s)$ будет, однако, не обязательно устойчивым, как показано в дальнейшем.

В качестве примера предположим, что принимаемый сигнал имеет вид

$$\sqrt{2}\, A_0 \sin[(\omega_0 + 2\pi f)\, t] + n(t), \tag{5.58}$$

где f — случайная частотная компонента со спектром $S_f(\omega) = 2\sigma^2_f\, \beta/(\omega^2 + \beta^2)$, а $\omega_0/2\pi$ — центральная частота ГУН. Тогда спектр фазы

$$S_\Phi(\omega) = \frac{2\sigma_f^2\, \beta}{\omega^2\, (\omega^2 + \beta^2)}.$$

Оптимальный фильтр $Y(i\omega)$ является сглаживающим фильтром, если сигнал имеет спектр $S_\Phi(\omega)$, а шум является белым со спектральной плотностью $S_n(\omega) = N_0/2A^2_0$. Так как шум является белым, а спектр сигнала рациональным (и асимптотически равным нулю), оптимальный фильтр определяется так же, как в ф-ле (5.28):

$$Y(i\,\omega) = 1 - \frac{(N_0/2A_0^2)^{1/2}}{\Psi(\omega)}. \tag{5.59}$$

Здесь $$|\Phi(\omega)|^2 = S_\Phi(\omega) + S_n(\omega) = \frac{N_0}{2A_0^2}\left[\frac{B_0^2 + a\, i\,\omega - \omega^2}{i\,\omega\,(i\,\omega + \beta)}\right] \times \left[\frac{B_0^2 - a\, i\,\omega - \omega^2}{i\,\omega\,(i\,\omega - \beta)}\right],$$

где $a = (2B^2_0 + \beta^2)^{1/2}$ и $B^4_0 = 4A^2_0\sigma^2_f\beta/N_0$. Следовательно,

$$Y(i\,\omega) = \left[\frac{B_0^2 + (a - \beta)\, i\,\omega}{B_0^2 + a\, i\,\omega - \omega^2}\right]. \tag{5.60}$$

Среднеквадратическая ошибка, обусловленная наличием шума, имеет вид [ср. с (5.31)]

$$\sigma_n^2 = \frac{1}{2\pi} \int\limits_{-\infty}^{\infty} \frac{N_0}{2A_0^2} |Y(\mathrm{i}\,\omega)|^2 d\omega = \frac{N_0 B_L}{A_0^2}, \tag{5.61}$$

где *ширина полосы системы ФАПЧ* $B_L = [B^2{}_0 + (a - \beta)^2]/4a$ равна ширине полосы идеального прямоугольного фильтра, который пропустил бы ту же самую мощность шума. Ошибка вследствие дрожания частоты равна

$$\sigma_s^2 = \frac{1}{2\pi} \int\limits_{-\infty}^{\infty} S_0(\omega) |1 - Y(\mathrm{i}\,\omega)|^2 d\omega = \frac{\sigma_f^2 \beta}{a B_0^2}. \tag{5.62}$$

Интересно отметить связь между полученной здесь фазовой ошибкой из-за наличия аддитивного шума (5.61) и соответствующим выражением при использовании оптимальной формулы оценки фазы, когда принимаемая фаза считается постоянной (см. § 3.7). Соответствующие выражения для ошибок в этих двух ситуациях: $\sigma^2{}_n = N_0 B_L/A^2{}_0$ и $\sigma^2{}_n = N_0/2A^2{}_0 T$ совпадают, если B_L и $1/2T$ равны. Напомним, что T — это время, в течение которого можно считать, что принимаемая синусоида имеет одну и ту же фазу, если производится оценка максимального правдоподобия.

В большинстве практических случаев наряду со случайными флуктуациями фазы генератора существуют переходные процессы из-за относительных различий между фазой принимаемого сигнала и фазой ГУН сигнала. Такой переходный процесс возникает, например, когда сигнал принимается впервые и цепь входит в синхронизм. Другой причиной возникновения переходного процесса может служить допплеровский сдвиг частоты принимаемого сигнала, приводящий к отклонению от центральной частоты цепи. Часто эти переходные процессы влияют намного сильнее, чем случайные колебания фазы, поэтому фильтры в системе часто выбираются единственно из тех соображений, чтобы избежать ошибок отслеживания из-за прогнозируемых переходных процессов. При этом фильтр ФАПЧ строится так, чтобы минимизировать среднеквадратическую ошибку, вызванную аддитивным шумом при заданной допустимой ошибке, возникающей из-за переходных процессов. Так же, как при анализе согласованных фильтров в § 5.3, процедура оптимизации, использующая этот критерий оптимальности, совпадает с процедурой, описанной для сглаживающего фильтра, если установить нужные соответствия.

Оптимизация при условии ограничения на переходные процессы выполняется следующим образом. Среднеквадратическая фазовая ошибка, вызванная аддитивным шумом,

$$\sigma_n^2 = \frac{1}{2\pi} \int\limits_{-\infty}^{\infty} |Y(\mathrm{i}\,\omega)|^2 S_n(\omega)\, d\omega, \tag{5.63}$$

где $S_n(\omega)=N_0/2A^2_0$, как раньше, — нормированная спектральная плотность шума. Ошибка из-за переходных процессов определяется как интеграл от квадрата разности между фазами на входе и выходе в отсутствие шума при условии, что переходный процесс начинается в момент $t=0$, т. е.

$$\sigma_T^2=\int_0^\infty[\Phi_1(t)-\Phi_0(t)]^2\,dt=\int_0^\infty\Phi_e^2(t)\,dt. \qquad (5.64)$$

Так как этот интеграл должен быть ограниченным, то существует, согласно теореме Планшереля, такая функция $\theta_e(\mathrm{i}\omega)$, что

$$\frac{1}{2\pi}\int_{-\infty}^{\infty}|\theta_e(\mathrm{i}\,\omega)|^2 d\,\omega=\int_{-\infty}^{\infty}\Phi_e^2(t)\,dt. \qquad (5.65)$$

Более того, если $\Phi_e(t)$ абсолютно интегрируема, что также желательно потребовать, то

$$\theta_e(\mathrm{i}\,\omega)=\int_{-\infty}^{\infty}\Phi_e(t)\,\mathrm{e}^{-\mathrm{i}\omega t}\,dt=\lim_{\alpha\to 0}\theta_e(s)=\lim_{\alpha\to 0}|\ 1-Y(s)\ |\ \theta_0(s), \qquad (5.66)$$

где снова $s=\alpha+\mathrm{i}\omega$.

Требуется минимизировать σ^2_n при наличии ограничений на переходную ошибку, т. е. отыскивается фильтр ФАПЧ, который минимизирует выражение

$$E^2=\sigma_n^2+\lambda^2\sigma_T^2\,. \qquad (5.67)$$

(Множитель Лагранжа λ определяется с помощью заданного уровня переходной ошибки, как сейчас будет показано.) Таким образом, требуется найти переходную функцию $Y(s)$, минимизирующую

$$E^2=\frac{1}{2\pi}\int_{-\infty}^{\infty}\{|\,Y(\mathrm{i}\,\omega)|^2S_n(\omega)+\lambda^2\ |\ Y(\mathrm{i}\,\omega)-1\,|^2\ |\ \theta_0(\mathrm{i}\,\omega)\ |^2\}\,d\,\omega. \qquad (5.68)$$

Но равенства (5.10) и (5.68) эквивалентны, если в первое вместо $S_z(\omega)$ подставить выражение $\lambda^2|\theta_0(\mathrm{i}\omega)|^2$ и если $S_{zn}(\omega)=0$. Поэтому оптимальные фильтры § 5.2 являются оптимальными и здесь.

Ясно, что самым важным переходным процессом при нашем рассмотрении является скачок частоты $\theta_0(s)=\Delta\omega/s^2$, так как центральные частоты передатчика и ГУН никогда не будут в точности равными. Систему ФАПЧ строят так, чтобы удержать ошибку отслеживания, возникающую из-за этого различия, в разумных пределах. Но так как

$$\lambda^2\ |\ \theta_0(\mathrm{i}\,\omega)\ |^2=\lim_{\beta\to 0}\frac{\lambda^2\,(\Delta\omega)^2}{\omega^2\,(\omega^2+\beta^2)}\,, \qquad (5.69)$$

то требуемое решение непосредственно вытекает из равенства (5.60), если подставить $\lambda^2(\Delta\omega)^2$ вместо $\sigma^2{}_f\beta$ и устремить β к нулю.

Оптимальная частотная характеристика системы ФАПЧ поэтому будет иметь вид

$$Y(\mathrm{i}\,\omega)=\frac{B_0^2+\sqrt{2}\,B_0\,\mathrm{i}\,\omega}{B_0^2+\sqrt{2}\,B_0\,\mathrm{i}\,\omega-\omega^2}\,, \tag{5.70}$$

где $B^4_0=[4A^2_0(\lambda\Delta\omega)^2]/N_0$. Как и ранее, средняя мощность шума на выходе может быть записана как

$$\sigma_n^2=\frac{1}{2\pi}\int\limits_{-\infty}^{\infty}\frac{N_0}{2A_0^2}\,|Y(\mathrm{i}\,\omega)|^2 d\,\omega=\frac{N_0B_L}{A_0^2}\ \text{рад}^2, \tag{5.71}$$

где $B_L=(3B_0/4\sqrt{2})$ — ширина полосы системы ФАПЧ.

Используя (5.57), где $A=A_0$, получим

$$H(s)=B_0^2+\sqrt{2}\,B_0 s/A_0Ks. \tag{5.72}$$

Таким образом, оптимальный фильтр зависит от B_0 и A_0 и, следовательно, от амплитуды сигнала, отношения сигнал/шум, абсолютной величины скачка частоты и значения λ, которое, в свою очередь, определяет величину переходной ошибки. Чтобы убедиться в этом, необходимо лишь заметить, что

$$e_T^2=\frac{1}{2\pi}\int\limits_{-\infty}^{\infty}|\theta_0(\mathrm{i}\,\omega)|^2\ |\ 1-Y(\mathrm{i}\,\omega)\,|^2\,d\,\omega\ =\frac{(\Delta\omega)^2}{(8B_L/3)^3}\ \text{рад}^2\ \text{с} \tag{5.73}$$

и ошибка обратно пропорциональна $\lambda^{3/2}$.

Если мощность сигнала A^2_1 и спектральная плотность шума N_1 отличаются от принятых при расчете значений A^2_0 и N_0, Вт/Гц, то дрожание фазы на выходе (в рад^2)

$$\sigma_n^2=\left(\frac{B_LN_1}{A_1^2}\right)\frac{1}{3}\left[2\,\frac{A_1}{A_0}\ +1\right] \tag{5.74}$$

и переходная ошибка (в рад^2 с)

$$e_T^2=\frac{(\Delta\omega)^2}{\left(\dfrac{8B_L}{3}\right)^3}\left(\frac{A_0}{A_1}\right)^2, \tag{5.75}$$

где B_L определено ранее.

Конечно, можно построить цепь так, чтобы компенсировать различные переходные процессы. Система ФАПЧ, изученная выше, часто называется *системой второго порядка*, так как $Y(s)$ имеет два полюса. *Система первого порядка* получается, если потребовать, чтобы переходные процессы, возникающие при скачке фазы

$$\theta_0(s)=\Delta\theta/s, \tag{5.76}$$

были ограниченными. В этом случае оптимальная передаточная функция, как легко видеть, имеет вид

$$Y(s)=4B_L/(s+4B_L), \tag{5.77}$$

тогда как

$$H(s) = 4B_L/A_0K, \tag{5.78}$$

где $B_L = \sqrt{2}\,\lambda(\Delta\theta)\,A_0/4N_0^{1/2}$.

Среднеквадратическая фазовая ошибка, обусловленная аддитивным шумом, и переходная ошибка (при произвольной амплитуде сигнала A_1 и спектральной плотности шума $N_1/2$) соответственно равны:

$$\sigma_n^2 = \frac{N_1B_L}{A_1^2}\left(\frac{A_1}{A_0}\right); \tag{5.79}$$

$$e_T^2 = \frac{(\Delta\theta^2)}{8B_L\,(A_1/A_0)}. \tag{5.80}$$

Для системы ФАПЧ *третьего порядка,* способной отслеживать линейные изменения частоты $\theta_0(s)=\Delta\alpha/s^3$, оптимальный фильтр ФАПЧ, оказывается, имеет вид

$$H(s) = \frac{\left(\frac{6}{5}B_L\right)^3 + 2\left(\frac{6}{5}B_L\right)^2 s + \frac{12}{5}B_L s^2}{A_0Ks^2}, \tag{5.81}$$

где $B_L^3 = \left(\frac{5}{6}\right)^3 \frac{\sqrt{2}\,\lambda(\Delta\alpha)\,A_0}{(N_0)^{1/2}}$.

Соответствующие ошибки для произвольных уровней сигнала и шума равны:

$$\sigma_n^2 = \frac{N_1B_L}{A_1^2}\,\frac{3}{5}\left[\frac{4\,(A_1/A_0)+1}{4\,(A_1/A_0)-1}\right]; \tag{5.82}$$

$$e_T^2 = \frac{\left(\frac{5}{6}\right)^3(\Delta\alpha)^2}{\left(\frac{A_1}{A_0}\right)\left[4\left(\frac{A_1}{A_0}\right)-1\right]B_L^3}. \tag{5.83}$$

Легко продемонстрировать преимущества системы ФАПЧ второго порядка. Если на входе системы ФАПЧ первого порядка возникает скачок частоты величины $\Delta\omega$, то фазовая ошибка

$$\Phi_e(t) = \frac{1}{2\pi\,\mathrm{i}}\int\limits_{-\mathrm{i}\,\infty}^{\mathrm{i}\,\infty}(1-Y(s))\,\frac{\Delta\omega}{s^2}\,\mathrm{e}^{st}\,ds = \frac{\Delta\omega}{4B_L}\left\{1-\mathrm{e}^{-4B_L t}\right\}$$

и $e(\infty)=\Delta\omega/4B_L$, так что остается нежелательная установившаяся ошибка. Система второго порядка дает при том же самом входе нулевую установившуюся ошибку. С другой стороны, так как разность частот двух генераторов, вообще говоря, не увеличивается (или уменьшается) бесконечно, то системы третьего порядка редко используются для синхронизации.

Итак, было показано, что с помощью соответствующим образом выбранных методов можно построить *отслеживающий* согласованный фильтр. Фильтр можно сконструировать так, чтобы скомпенсировать случайные флуктуации фазы или с равным успехом переходные процессы (или и то, и другое одновременно). К сожалению, оптимальный фильтр в общем случае зависит от отношения сигнал/шум. В частности, показано, что ширина полосы оптимальной цепи в каждой из трех только что рассмотренных систем ФАПЧ прямо пропорциональна некоторой дробной степени отношения сигнал/шум. Однако если параметры фильтра не изменяются при изменении отношения сигнал/шум на входе, то эффективная ширина полосы системы ФАПЧ — функция лишь амплитуды сигнала [см. равенства (5.74), (5.75), (5.78), (5.79) и (5.82), (5.83)]. В результате, хотя в каждой из этих систем среднеквадратическая ошибка фазы и переходная ошибка уменьшаются, когда мощность сигнала возрастает по сравнению со значением, принятым при расчете, но они не уменьшаются пропорционально, как в случае фильтра ФАПЧ, оптимизированного для каждого уровня сигнала.

На практике системам ФАПЧ обычно предшествуют полосовые ограничители или устройства автоматической регулировки усиления. Благодаря этим устройствам полоса цепи зависит от отношения сигнал/шум, а не от уровня сигнала, и, следовательно, зависимость от этих параметров более близка к оптимальному случаю. Это утверждение является прямым следствием двух особенностей полосовых ограничителей и устройств автоматической регулировки усиления:

1. Отношение сигнал/шум S'_1/N'_1B_1 на выходе таких приборов прямо пропорционально отношению S_1/N_1B_1 на их входе, т. е. $S'_1/N'_1B_1 = kS_1/N_1B_1$, где $\pi/4 < k < 2$ для полосовых ограничителей с шириной полосы B_1 [1] и, по-видимому, $k=1$ для устройств автоматической регулировки усиления.

2. Полная мощность на выходе таких устройств постоянна независимо от отношения сигнал/шум на входе, т. е. $S'_1 + N'_1B_1 = K$.

Таким образом, $S'_1 = K \dfrac{S_1}{S_1 + N_1B_1/k}$ и $N'_1 = \dfrac{K}{k}\,\dfrac{N_1}{S_1 + N_1B_1/k}$.

В соответствии с этим увеличение уровня принятого сигнала частично проявляется на входе цепи как уменьшение уровня шума. Ширина полосы системы поэтому с ростом уровня сигнала увеличивается медленнее (и, следовательно, она ближе к оптимальному случаю), чем в отсутствие ограничителя. Аналогично увеличение уровня шума проявляется частично как уменьшение мощности сигнала на входе цепи. Это, в свою очередь, приводит к уменьшению ширины полосы цепи, что ближе к идеальной ситуации.

В любом случае обычно принято строить цепь так, чтобы работать оптимально в наихудших ожидаемых условиях. Хотя работа и не будет оптимальной для других уровней, отличных от номинального, она все же будет лучше, чем в этом крайнем случае, в котором работа считается удовлетворительной.

---

[1] См. задачу 5.6.

В общем случае случайные флуктуации фазы (шум генератора) присутствуют, даже когда цепь строится так, чтобы компенсировать лишь аддитивный шум и ожидаемые переходные процессы. Шум генератора увеличивает среднеквадратическую ошибку по сравнению с пределом, который соответствует лишь аддитивному шуму. Тем не менее в большинстве случаев полоса системы ФАПЧ, необходимая для того, чтобы сделать приемлемыми переходные процессы, достаточно широка, чтобы сделать влияние шума генератора относительно малым по сравнению с влиянием аддитивного шума. Это предположение будет использоваться в последующем анализе систем ФАПЧ.

Анализ, проведенный в этом параграфе, начинался с предположения, что линейная модель дает хорошее приближение к действительному поведению системы ФАПЧ. Экспериментальные результаты показывают, что это имеет место, когда среднеквадратическая ошибка отслеживания цепи не превышает 1/4 рад^2. Нелинейный анализ цепи первого порядка приводит к результатам, которые очень близко согласуются с результатами линейного анализа в том же интервале ошибок. Другие приближенные нелинейные подходы также подтверждают этот вывод для цепей более высокого порядка. Во всех применениях, с которыми мы будем сталкиваться, среднеквадратическая ошибка фазы, большая, чем 1/4 рад^2, будет недопустимой. В соответствии с этим линейная модель будет, как правило, приемлемой для наших целей. Исключением из этого правила является начальный процесс входа в синхронизм, когда система еще не отслеживает принимаемый сигнал. Эта сторона задачи обсуждается в следующем параграфе.

5.7. Время входа в синхронизм

В этом параграфе получим оценки для времени, необходимого для того, чтобы привести систему ФАПЧ в состояние синхронизма¹), когда начальная разность между частотой ГУН и частотой принимаемого сигнала равна Δf. Так как два независимых генератора никогда не будут работать точно на одной и той же частоте, эта задача неизбежно возникает в начальной стадии процесса входа в синхронизм. Система ФАПЧ второго порядка способна отследить такой сдвиг частот с нулевой установившейся ошибкой; системы ФАПЧ более высокого порядка также обладают этим свойством, но так как для них возникает проблема устойчивости, когда параметры сигнала отличаются от номинальных значений, то, вообще говоря, системы второго порядка предпочтительнее. Более того, как уже было отмечено, те переходные процессы, которые требуют введения цепей более высокого порядка, имеют, как правило, ограниченную продолжительность. По этим

---

¹) Говорят, что цепь синхронизации фазы будет в «состоянии синхронизма», когда разность фаз между сигналом ГУН и принимаемым сигналом становится и продолжает оставаться меньше, чем π рад. (*Прим. авт.*).

причинам ограничим наше внимание изучением процесса входа в синхронизм лишь системы ФАПЧ второго порядка в случае, когда первоначальный сдвиг частоты равен постоянной Δf.

Вычисление времени, необходимого для вхождения в синхронизм при использовании системы ФАПЧ, хотя и несомненно связано с поведением цепи в состоянии синхронизма, является по своему существу более трудным для анализа. Дело в том, что здесь нельзя использовать линейную модель системы ФАПЧ; очевидно, что до того, как произойдет захватывание, система должна вообще говоря, работать за пределами линейного участка диапазона. Ниже получены некоторые приближенные результаты, в случае, когда можно пренебречь шумом на входе системы. Так как оценки фазы должны быть довольно точными для того, чтобы их можно было использовать в синхронных системах, интерес представляет случай с большим значением отношения сигнал/шум. Поэтому время входа в синхронизм системы в отсутствие шума будет разумной оценкой ее характеристик в большинстве приложений, связанных с синхронизацией.

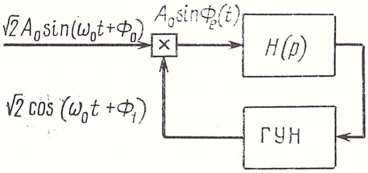

$\sqrt{2}A_0\sin(\omega_0 t+\Phi_0)$
$A_0\sin\Phi_e(t)$
×
$H(p)$
$\sqrt{2}\cos(\omega_0 t+\Phi_1)$
ГУН

Рис. 5.6. Функциональная схема нелинейной модели системы ФАПЧ

Для анализа времени входа в синхронизм вернемся к нелинеаризованной модели системы ФАПЧ (рис. 5.6). Высокочастотные составляющие на выходе умножителя могут не приниматься во внимание, так как они опять-таки будут, фактически, устранены фильтром. Фильтр $H(p)$ уже был найден (p обозначает оператор d/dt), так что анализ можно провести во временно́й области. Выходная частота ГУН состоит из постоянной составляющей ω_0, т. е. центральной частоты, и составляющей, пропорциональной напряжению на входе $H(p)A_0\sin\Phi_e(t)$. Поэтому $\Phi_1(t)=(K_0H(p)/p)\times\times A_0\sin\Phi_e(t)$, где K_0 — постоянная, обозначающая коэффициент усиления ГУН, и

$$\Phi_0(t)-\Phi_1(t)=\Phi_0(t)-\frac{H(p)A_0K_0}{p}\sin\Phi_e(t)=\Phi_e(t). \tag{5.84}$$

Дифференцируя, находим

$$\frac{d\Phi_e(t)}{dt}+H(p)A_0K_0\sin\Phi_e(t)=\frac{d\Phi_0(t)}{dt}=\Delta_\omega, \tag{5.85}$$

последнее равенство следует из того, что первоначальная разность частот ГУН и принимаемого сигнала по предположению равна $\Delta\omega$ рад/с; $\Phi_0(t)=(\Delta\omega)t+\Phi_0$. Характеристика фильтра системы второго порядка, который был введен в § 5.6, имела вид

$$H(p)=K_1(1+\tau_0 p)/p. \tag{5.86}$$

(Для оптимального фильтра в соответствии с критерием § 5.6 $K_1=B^2{}_0/A_0K_0$ и $\tau_0=\sqrt{2}/B_0$.) Подставляя $H(p)$ в (5.85) и опять дифференцируя, получаем

$$\frac{d^2\Phi_e}{dt^2} + \frac{d\Phi_e}{dt}\tau_0 K\cos\Phi_e + K\sin\Phi_e = \frac{d^2\Phi_0(t)}{dt^2}, \tag{5.87}$$

где $K = A_0K_0K_1$. Предполагается, что частота на входе постоянна, так что $d^2\Phi_0(t)/dt^2 = 0$. Удобно сделать подстановку $\tau = \tau_0 Kt$. Тогда равенство (5.84) упростится и примет вид

$$\frac{d^2\Phi_e}{d\tau^2} + \cos\Phi_e\frac{d\Phi_e}{d\tau} + \frac{1}{K\tau_0^2}\sin\Phi_e = \dot f + f\cos\Phi + \frac{1}{K\tau_0^2}\sin\Phi = 0, \tag{5.88}$$

где $\Phi = \Phi_e(t)$; $f = \frac{d\Phi_e(t)}{d\tau}$ и $\dot f = \frac{d^2\Phi_e(t)}{d\tau^2}$.

Таким образом,

$$\frac{\dot f}{f} = \frac{df}{d\tau}\Big/\frac{d\Phi}{d\tau} = \frac{df}{d\Phi} = -\cos\Phi - \frac{\sin\Phi}{4\zeta^2 f}, \tag{5.89}$$

где $\zeta^2 = K\tau_0^2/4$.

Равенство (5.89) можно использовать, чтобы получить приближенное выражение для времени входа в синхронизм. С этой целью умножим обе части (5.89) на $\sin\Phi d\Phi$ и проинтегрируем в пределах от $\Phi = 2\pi k$ до $\Phi = 2\pi(k+1)$, где k — произвольное целое число; в результате получим

$$\int\limits_{\Phi=2\pi k}^{\Phi=2\pi(k+1)}\sin\Phi\, df = -\int\limits_{2\pi k}^{2\pi(k+1)}\frac{\sin^2\Phi}{4\zeta^2 f}d\Phi = -\int\limits_{2\pi k}^{2\pi(k+1)} f\cos\Phi\, d\Phi, \tag{5.90}$$

где последний интеграл получен при интегрировании по частям первого интеграла. Аналогично умножая обе части (5.89) на $fd\Phi$, интегрируя в тех же пределах и используя ф-лу (5.87), получим

$$\frac{1}{2}[f^2(2\pi(k+1)) - f^2(2\pi k)] = -\int\limits_{2\pi k}^{2\pi(k+1)} f\cos\Phi\, d\Phi = -\int\limits_{2\pi k}^{2\pi(k+1)}\frac{\sin^2\Phi}{4\zeta^2 f}d\Phi. \tag{5.91}$$

Если функция f положительна, то последний интеграл положителен, и тот факт, что $f[2\pi(k+1)] < f(2\pi k)$, означает, что независимо от величины разности частот f каждый полный цикл приводит к уменьшению этой разности. Если f отрицательна, что соответствует изменению направления отсчета фазы на противоположное [от $2\pi(k+1)$ к $2\pi k$ рад], то интеграл справа отрицателен и $|f(2\pi k)| < |f[2\pi(k+1)]|$. Разность частот, таким образом, стремится к нулю независимо от первоначального значения. Теоретически частотный диапазон захвата бесконечен.

Чтобы оценить время, необходимое для входа в синхронизм, напомним, что $f = d\Phi/d\tau$ и, следовательно,

$$t = \frac{\tau}{\tau_0 K} = \frac{1}{\tau_0 K}\int\frac{d\Phi}{f}. \tag{5.92}$$

Суммируя равенство (5.91) по n периодам, находим, что

$$f_2(2\pi n) - f^2(0) = -\frac{1}{2\zeta^2}\int\limits_0^{2n\pi} \frac{\sin^2\Phi}{f}\,d\Phi.$$

Для некоторого значения n имеем $f^2(2n\pi) \approx 0$ и

$$f^2(0) - f^2(2\pi n) = \frac{1}{2\zeta^2}\int\limits_0^{2\pi n} \frac{\sin^2\Phi}{f}\,d\Phi = \frac{\alpha}{2\zeta^2}\int\limits_0^{2\pi n} \frac{d\Phi}{f} = \frac{2T_{\Delta f}\,\alpha}{\tau_0}, \tag{5.93}$$

где $T_{\Delta f}$ — время, необходимое для того, чтобы разность частот стала приближенно равной нулю в случае, когда начальная разность равна $\Delta f = [\tau_0 K f(0)/2\pi]$ Гц; α — некоторое число из интервала $0 < \alpha < 1$. Поэтому

$$T_{\Delta f} = \frac{\pi^2}{8\alpha\zeta}\left(\frac{1 + 4\zeta^2}{4\zeta}\right)^3 \frac{(\Delta f)^2}{B_L^3}, \tag{5.94}$$

где $T_{\Delta f}$ дано в секундах; $B_L = (1/4\tau_0)(1 + 4\zeta^2)$ — ширина полосы системы ФАПЧ в случае, когда фильтр ФАПЧ задается равенством (5.86). [Если используется оптимальный фильтр, введенный в § 5.6, то $\zeta^2 = 1/2$ и $\tau_0 = \sqrt{2}/B_0$. Интересно отметить, что время входа в синхронизм согласно ф-ле (5.94) в действительности минимизируется, когда $\zeta^2 = 1/2$]. Хорошая в общем случае оценка для $T_{\Delta f}$ получается, когда $\sin^2 x$ в (5.93) заменяется на его среднее значение 1/2. Тогда $\alpha = 1/2$ и

$$T_{\Delta f} \approx \frac{\pi^2}{4\zeta}\left(\frac{1 + 4\zeta^2}{4\zeta}\right)^3 \frac{(\Delta f)^2}{B_L^3}. \tag{5.95}$$

В некоторых случаях возможно (и желательно) увеличивать B_L во время входа в синхронизм для того, чтобы уменьшить требуемое время, и уменьшать B_L после входа в синхронизм. Однако величина, на которую можно изменить B_L, ограничена шумом, так как увеличение ширины полосы системы усиливает влияние аддитивного шума и, следовательно, общую вероятность неудачи при входе в синхронизм.

Мы установили, что время, необходимое для входа в синхронизм, растет как квадрат разности частот ГУН и принимаемого сигнала. Когда начальная разность частот велика, время входа в синхронизм может быть чрезмерно большим. В этом случае широко применяется метод, который состоит в подаче на вход ГУН дополнительного линейно возрастающего (или убывающего) напряжения, что приводит к качанию частоты ГУН в интервале неопределенности. Предыдущие рассуждения можно обобщить так, чтобы получить некоторые предельные результаты для этого случая. В силу того что

$$\Phi_1(t) = \frac{K_0 H(p)}{p} A_0 \sin\Phi_e(t) - \frac{1}{2}\beta t^2, \tag{5.96}$$

где β — скорость качания, рад/с^2, равенство (5.85) принимает вид

$$\frac{d\Phi_e(t)}{dt} + A_0K_0H(p)\sin\Phi_e(t) = \frac{d\Phi_0(t)}{dt} + \beta t. \tag{5.97}$$

Подстановка $H(p)$ и дифференцирование, как и ранее, дают

$$\frac{d^2\Phi_e}{dt^2} + \frac{d\Phi_e}{dt}\tau_0K\cos\Phi_e + K\sin\Phi_e = \frac{d^2\Phi_0(t)}{dt^2} + \beta \tag{5.98}$$

вместо (5.87). Равенство (5.89) принимает вид

$$\frac{df}{d\Phi} = -\cos\Phi + \frac{\beta/K - \sin\Phi}{4\zeta^2 f}. \tag{5.99}$$

Интегрируя обе части этого равенства в пределах от $2\pi k$ до $2\pi(k+1)$, получаем

$$f(2\pi(k+1)) - f(2\pi k) = \frac{1}{4\zeta^2}\int\limits_{2\pi k}^{2\pi(k+1)} \frac{\beta/K - \sin\Phi}{f}\,d\Phi. \tag{5.100}$$

Но теперь, если $\beta > K$, то положительное значение f в течение любого одного цикла означает, что $f[2\pi(k+1)]$ больше, чем $f(2\pi k)$, в то время как отрицательная разность частот означает, что $f(2\pi k) < f(2\pi(k+1))$, когда $\beta < -K$. В любом из этих случаев разность частот растет по абсолютной величине на любом единичном цикле. Более того, когда f мало по абсолютной величине, равенство (5.99) показывает, что f будет возрастающей функцией Φ, если $f > 0$ и $\beta > K$ и если $f < 0$ и $\beta < -K$. Соответственно абсолютное значение f является возрастающей функцией времени при малых значениях f. Эти два фактора заведомо приводят к неустойчивости системы, если β по абсолютной величине превосходит K; как следствие, вхождение в синхронизм оказывается невозможным. Экспериментальные данные и моделирование на вычислительной машине подтверждают этот вывод наряду с несколько более слабым обратным утверждением, что при $|\beta| < K/2$ захватывание имеет место. (При малых отношениях сигнал/шум $|\beta|$ должно быть меньше K. Однако при отношениях сигнал/шум, часто имеющих место при когерентной связи и в задачах синхронизации, $|\beta|$ может быть близко к $K/2$.)

Время, необходимое для качания частоты в интервале неопределенности Δf Гц со скоростью $\beta/2\pi$ Гц/с, равно $2\pi\Delta f/\beta$ секунд. Время входа в синхронизм при использовании этого метода

$$T'_{\Delta f} = \frac{2\pi\Delta f}{\beta} \approx \frac{4\pi\Delta f}{K} = \frac{\pi\Delta f}{[4\zeta/(1+4\zeta^2)]^2 B_L^2}. \tag{5.101}$$

Сравнивая ф-лы (5.101) и (5.95), находим, что качание частоты ГУН в области неопределенности становится эффективным, если

$$\Delta f > \frac{4}{\pi}\,\frac{4\zeta^2}{1+4\zeta^2}B_L. \tag{5.102}$$

Эти оценки времени входа в синхронизм не учитывают время, в течение которого фазовая ошибка уменьшается до некоторого достаточно малого значения после того, как частотная ошибка была устранена. Чтобы оценить эту величину, рассмотрим случай, когда цепь первоначально находится в синхронизме, но фаза принимаемого сигнала изменяется скачком на величину $\Delta\theta$ в момент $t=0$. Если $\Delta\theta$ не слишком велико, то опять может быть использована линейная модель системы ФАПЧ. Так как мы рассматриваем систему второго порядка, то имеем

$$\theta_e(t) = \frac{1}{2\pi i}\int\limits_{-i\infty}^{i\infty} \frac{\Delta\theta}{s}[1 - Y(s)]e^{st}\,ds = \sqrt{2}\,\Delta\theta\, e^{-B_0 t/\sqrt{2}} \cos\left(\frac{\sqrt{2}\,B_0 t}{2} + \frac{\pi}{4}\right).$$

Время, необходимое для того, чтобы огибающая этой переходной ошибки уменьшилась приближенно до 1/4 ее первоначального значения, равно, следовательно, $T \; = 1/B_L$. Это, конечно, дает лишь грубую оценку интересующей нас величины. Тем не менее, если величина B_L мала по сравнению с неопределенностью частоты Δf, то эта добавка к общему времени входа в синхронизм, по-видимому, пренебрежимо мала по сравнению со временем, необходимым, чтобы отследить первоначальный сдвиг частоты [(5.95) или (5.101)].

5.8. Системы ФАПЧ и несинусоидальные сигналы

Рассмотрение, которое привело к формулировке понятия системы ФАПЧ в § 5.4, без особого обоснования ограничивалось синусоидальными сигналами. Тот же подход в равной мере применим к любому периодическому сигналу $x(t)$. Так как выход генератора сигнала (рис. 5.1 и рис. 5.2) обозначен через $x'(t)$, то это утверждение можно понять в том смысле, что обобщение производится лишь на дифференцируемые периодические функции. Однако в действительности это не является необходимым. Такое же устройство можно было бы предложить для отслеживания фазы сигнала $x(t)$ при использовании некоторого местного периодического сигнала, отличного от $x'(t)$. Рассуждения § 5.4, которые привели к обоснованию системы ФАПЧ, изображенной на рис. 5.2, в равной мере применимы и тогда, когда местный сигнал является любой периодической функцией $z(t)$, такой, что

$$\int\limits_0^T x(t)\,z(t+\tau)\,dt\,\Big|_{\tau=0} = 0; \tag{5.103}$$

$$\frac{\partial}{\partial\tau}\int\limits_0^T x(t)\,z(t+\tau)\,dt\,\Big|_{\tau=0} < 0,$$

причем оба этих условия выполняются лишь в точке $\tau=0$. В действительности, используя некоторый местный сигнал $z(t)$, отличный от $x'(t)$, можно было бы получить, по-видимому, существенно лучшие характеристики отслеживания. Вскоре мы возвратимся к этому вопросу.

Для того чтобы рассмотрение было по возможности наиболее общим, предположим, что местный сигнал $z(t)$ является периодической функцией, в остальном неопределенной. Однако $z(t)$ и $x(t)$ будут нормированы так, чтобы их мощность была равна единице. Так как амплитуда A принимаемого сигнала произвольна и так как увеличение амплитуды сигнала $z(t)$ эквивалентно, например, увеличению усиления цепи, то такая нормировка не приводит к потере общности.

Тогда, если условия, приводящие к системе ФАПЧ, выполнены (т. е. если τ и $\hat{\tau}$ — относительно медленно изменяющиеся функции времени), система ФАПЧ и устройство слежения, изображенное на рис. 5.1, являются эквивалентными. В этих условиях влияние принимаемого сигнала $x(t+\tau)$ на характеристику системы зависит всецело от корреляционной функции

$$\rho_{xz}(\hat{\tau}-\tau) = \frac{1}{T}\int_{0}^{T} x(t+\tau)\,z(t+\hat{\tau})\,dt. \tag{5.104}$$

Более того, если с достаточно большой вероятностью можно сказать, что система работает в достаточно малой области вблизи точки $\hat{\tau}=\tau$, то

$$\rho_{xz}(\tau-\hat{\tau}) \approx (\tau-\hat{\tau})\,\lambda, \tag{5.105}$$

где $\lambda = \frac{d}{d\tau}\rho_{xz}(\tau)\big|_{\tau=0} \overset{\Delta}{=} \rho'_{xz}(0)$.

(Это, конечно, как раз то приближение, которое привело к линейной системе в § 5.5.) Оказывается, таким образом, что пока ошибка отслеживания остается в пределах этой ограниченной области, влияние вида функции, которая описывает принимаемый сигнал, проявляется лишь с помощью величины $\rho'_{xz}(0)$, так что все сигналы $x(t)$ и $z(t)$ с одинаковым параметром $\rho'_{xz}(0)$ являются эквивалентными.

Однако, чтобы обосновать утверждение, что существенна только корреляционная функция $\rho'_{xz}(\tau)$ или (в линейной области) производная этой корреляционной функции, необходимо также заново исследовать произведение $z(t+\hat{\tau})n(t)$, описывающее шум на входе фильтра ФАПЧ. Фаза $\hat{\tau}=\hat{\tau}(t)$ зависит от шума $n(t_1)$, но, как и в § 5.5, только при $t_1<t$. Таким образом, утверждение, что спектр этого произведения является «белым», если $n(t)$ занимает полосу, бо́льшую, чем полоса системы, остается справедливым. Если двусторонняя спектральная плотность мощности процесса $n(t)$ равна

$N_0/2$, то спектральная плотность процесса $z(t+\hat{\tau})n(t)$ согласно § 5.5 имеет вид

$$\frac{N_0}{2}E[z^2(t+\hat{\tau})]=\frac{N_0}{2}\,. \qquad (5.106)$$

Рассмотрим далее распределение амплитуды низкочастотных компонент произведения $z(t+\hat{\tau})n(t)$ в какой-либо момент времени. (Высокочастотные компоненты снова будут устранены благодаря фильтрации, которую выполняет цепь.) Для этого разложим периодический сигнал $z(t+\hat{\tau})$ в ряд Фурье:

$$z(t+\hat{\tau})=\sum_{i=0}^{\infty}a_i\cos(\omega_i t+\theta_i);\quad \omega_i=\frac{2\pi i}{T}\,.$$

Временно введем перед системой ФАПЧ параллельно соединенные идеальные полосовые фильтры, центральная частота каждого из которых равна одной из гармонических частот $\omega_i=2\pi i/T$, $i\geqslant 0$ и каждый из которых имеет одну и ту же ширину полосы $B\leqslant 1/T$ (за исключением полосы около нулевой частоты, которая равна половине этой величины). Как и в § 5.5, шум на выходе i-го фильтра можно записать в виде

$$n_i(t)=n_{c_i}(t)\cos\omega_i t-n_{s_i}(t)\sin\omega_i t. \qquad (5.107)$$

Тогда

$$\{z(t+\hat{\tau})n(t)\}_{lf}=\left\{\sum_{i,\,j}a_i\cos(\omega_i t+\theta_i)\,[n_{c_j}(t)\cos\omega_j t-n_{s_j}(t)\sin\omega_j t]\right\}_{lf}=$$

$$=\sum_{i=1}^{\infty}\frac{a_i}{2}\,[n_{c_i}(t)\cos\theta_i+n_{s_i}(t)\sin\theta_i]+a_0 n_{c_0}(t). \qquad (5.108)$$

Это выражение представляет собой просто взвешенную сумму членов вида, определяемого равенством (5.53); как было показано, эти члены являются гауссовскими случайными величинами с нулевыми средними и с не зависящими от времени вторыми моментами. Цель рассмотрения системы ФАПЧ с полосовыми фильтрами — получить удобное представление для шума. Но рассуждения, приводящие к (5.108), справедливы даже тогда, когда $B=1/T$, т. е. когда в действительности вообще нет никаких фильтров. Поэтому заключаем, как в § 5.5, что низкочастотная компонента шума на входе фильтра цепи является выборочной функцией белого (т. е. широкополосного по сравнению с полосой системы) гауссовского случайного процесса.

Если $z(t)$ — прямоугольная функция, принимающая значения только $+1$ и -1, то утверждение, что $n(t)z(t)$ имеет то же самое распределение, что и $n(t)$, когда $n(t)$ является белым и симметрично распределенным процессом, очевидно. Распределения процессов $n(t)$ и $-n(t)$ в точности совпадают, и так как $n(t)$ и $n(t+\varepsilon)$ независимы при всех $\varepsilon\neq 0$, то невозможно определить, наблюдается ли $n(t)$ или $-n(t)$. Статистические характеристики шума остаются, очевидно, в этом случае неизменными. Предыдущие рассуждения показывают, что тот же самый вывод справедлив для низкочастотных компонент произведения $n(t)z(t)$, где $z(t)$ — любая периодическая функция. Как подсказывает интуиция, $\{z(t)n(t)\}$ — сдвинутый по частоте белый шум, и этот сдвиг не меняет никаких свойств, потому что шум белый.

Объединяя эти два факта [т. е. (во-первых), что статистические свойства шума $n_1(t)=\{n(t)z(t+\hat{\tau})\}_{lf}$ фактически не зависят от $z(t)$ и (во-вторых), что сигнал ошибки в линейной модели цепи зависит не от самого сигнала $z(t)$, а от производной корреляционной функции $\rho_{xz}(\tau)$], приходим к следующему выводу. Характеристика системы ФАПЧ, построенной для слежения за произвольным периодическим сигналом $Ax(t)$ с периодом T, совпадает с характеристикой системы, имеющей синусоидальный вход (как предсказывала нелинейная модель), когда корень квадратный из среднеквадратического значения амплитуды синусоиды

$$A_{\text{в}}=\frac{AT}{2\pi}\left|\rho'_{xz}(0)\right| . \tag{5.109}$$

Это заключение верно, пока система ФАПЧ работает в области, в которой производная корреляционной функции $\rho_{xz}(\tau)$ относительно постоянна.

Возвращаясь к вопросу о том, нужно ли $z(t)$ приравнивать $x'(t)$, как предлагается в рассуждениях § 5.4, заметим, что «наилучшим» с точки зрения равенства (5.109) является такой выбор $z(t)$, который дает корреляционную функцию с максимальной возможной производной в окрестности $\tau=0$. Поэтому оптимальный выбор $z(t)$ равен $x'(t)$. Действительно,

$$\rho'_{xz}(0)|=\left|\frac{\partial}{\partial\tau}\frac{1}{T}\int_0^T x(t)\,z(t+\tau)\,dt\right|_{\tau=0}=\left|\frac{1}{T}\int_0^T x(t)\,z'(t)\,dt\right|. \tag{5.110}$$

Интегрируя это выражение по частям и используя неравенство Шварца, находим, что

$$|\rho'_{xz}(0)|=\left|\frac{1}{T}\int_0^T [x'(t)z(t)\,dt\right|\leqslant\left[\frac{1}{T}\int_0^T [x'(t)]^2\,dt\right]^{1/2}\left[\frac{1}{T}\int_0^T z^2(t)dt\right]^{1/2}. \tag{5.111}$$

Но так как $z(t)$ по условию имеет единичную мощность, правая часть неравенства не зависит от этой функции. Сформулированный вывод справедлив в силу того, что это неравенство переходит в равенство тогда и только тогда, когда $z(t)=kx'(t)$ для некоторой постоянной k. Фактически, этот результат прямо связан с эффективностью формулы оценки максимального правдоподобия величины τ [см. ф-лу (5.39)].

Это, однако, не все, что можно сказать, так как система ФАПЧ не всегда будет работать в линейной области около точки $\tau=0$, особенно, если эта область мала. В предшествующем абзаце установлено, что оптимальный местный сигнал $z(t)$ для заданного принимаемого сигнала $x(t)$ имеет вид $z(t)=x'(t)$ *при условии*, что корреляционная функция $\rho_{xx'}(\tau)$ приближенно является линейной функцией τ в достаточно большой окрестности точки $\tau=0$[1]).

Чтобы сделать в какой-то мере более определенными рассуждения относительно важности расширения линейной области, предположим, что $\rho_{xz}(\tau)$ — строго линейная функция τ для $|\tau|<L/2$ и что фаза принимаемого сигнала постоянна. Тогда в соответствии с линейной моделью вероятность того, что ошибка отслеживания для системы ФАПЧ $\tau_e=\tau-\hat{\tau}$ останется в пределах этой области[2]),

$$\Pr\left\{|\tau_e|<\frac{L}{2}\right\}=\operatorname{erf}\left(\frac{\pi L}{2\sigma_\Phi T}\right), \tag{5.112}$$

где $\sigma_\Phi^2=N_0B_L/A_e$. Если $\rho_{xz}(\tau)$ не является строго линейной функцией τ в области $|\tau|\leqslant L/2$, а имеет вид, изображенный на рис. 5.7, то все еще справедливо равенство

$$\Pr\left(|\tau_e|<\frac{L}{2}\right)=\operatorname{erf}\left(\frac{\pi Lk(L)}{\sqrt{2}\,\sigma_\Phi T}\right) \tag{5.113}$$

для некоторого $k(L)$ из интервала $\lambda(L)/\lambda_0\leqslant k(L)\leqslant 1$, где $\lambda(L)$ определена на рис. 5.7. Значение этой вероятности, рассматриваемой

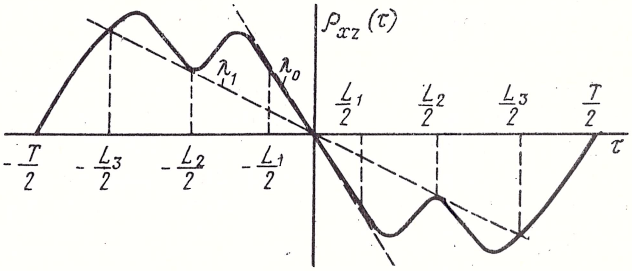


Рис. 5.7. Пример корреляционной функции и связанных с нею границ

$$\lambda(L)=\begin{cases}\lambda_0, & |\tau|\leqslant\dfrac{L_1}{2};\\[2ex] \dfrac{\rho_{xz}}{\tau}, & \dfrac{L_1}{2}\leqslant|\tau|\leqslant\dfrac{L_2}{2},\quad \dfrac{L_3}{2}\leqslant|\tau|\leqslant\dfrac{\tau}{2};\\[2ex] \lambda_1, & \dfrac{L_2}{2}\leqslant|\tau|\leqslant\dfrac{L_3}{2}\end{cases}$$

---

[1]) Так как производная синусоиды в разумном приближении является линейной на значительной доле ее периода, то местный сигнал [если $x(t)$ — синусоида] должен, по-видимому, также быть синусоидой, как предполагалось в предыдущих параграфах. Даже здесь, однако, другие критерии могли бы привести к другим выводам. Если бы считалось более важным, например, расширить область линейности функции $\rho_{xz}(\tau)$, то для того, чтобы максимизировать $\rho'_{xz}(0)$, можно было бы произвести другой выбор $z(t)$. *(Прим. авт.)*.

[2]) Так как в предположениях, которые используются здесь, ошибка отслеживания является линейной функцией гауссовского случайного процесса (ср. с § 5.5), она сама является гауссовским случайным процессом. *(Прим. авт.)*.

как функция L, определяет меру адекватности линейной модели системы ФАПЧ для какой-либо частной рассматриваемой задачи.

Те же рассуждения можно использовать для оценки вероятности потери синхронизма. В силу того что по определению потери синхронизма возникают всегда, когда $|\tau_e| > T/2$, то

$$p \triangleq \Pr(\text{потеря синхронизма}) = \Pr\left\{|\tau_e| > \frac{T}{2}\right\} = 1 - \operatorname{erf}\left(\frac{\pi k}{\sqrt{2}\,\sigma_\Phi}\right) \tag{5.114}$$

для некоторого k; $\max\limits_{L \leqslant T} L\lambda(L)/\lambda_0 T \leqslant k \leqslant 1$. Если независимые выборки ошибки отслеживания берутся до того, как была обнаружена потеря синхронизма, то математическое ожидание числа требуемых выборок

$$E(n) = \sum_{n=1}^{\infty} n(1-p)^n p = 1/p. \tag{5.115}$$

В силу того что минимальный временно́й интервал, разделяющий независимые выборки на выходе цепи, имеет порядок $1/2B_L$, математическое ожидание времени до потери синхронизма

$$\overline{T} = \frac{E(n)}{2B_L} \approx \frac{1}{2B_L\left[1 - \operatorname{erf}\left(\dfrac{\pi k}{\sqrt{2}\,\sigma_\Phi}\right)\right]}. \tag{5.116}$$

Хотя это рассуждение полностью эвристическое, его справедливость может быть подтверждена для систем первого порядка с помощью нелинейной модели. Если, например, $\rho_{xz}(\tau)$ — синусоида, то среднее время до потери синхронизма для системы первого порядка хорошо аппроксимируется для всех $\sigma_\Phi < 1/2$ рад равенством (5.116), где $k = 2/\pi$.

Задачи

5.1. Сигнал $y(t) = x(t) + n(t)$ проходит через два сглаживающих фильтра, построенных так, чтобы минимизировать среднеквадратические оценки $\hat{x}(t)$ и $\hat{n}(t)$ для $x(t)$ и $n(t)$ соответственно.

а) Сравнить две оценки $\hat{x}(t)$ и $y(t) - \hat{n}(t)$ для $x(t)$.

б) Выразить $\hat{y}(t) \triangleq \hat{x}(t) + \hat{n}(t)$ через $x(t)$ и $n(t)$.

5.2. Проверить равенства (5.77)—(5.83).

5.3. Фильтр системы второго порядка, определенный ф-лой (5.72), имеет вид $H(s) = a + (b/s)$ и, следовательно, включает в себя идеальный интегратор. На практике интегратор не будет идеальным и фильтр будет иметь вид $H(s) = (as + b)/(s + \delta)$, где δ мала, но не равна нулю. Определить ширину полосы шума системы с таким фильтром, найти установившийся отклик системы на единичный частотный скачок.

5.4. Показать, используя, например, метод корневого годографа, что линейные модели системы ФАПЧ первого и второго порядков (с идеальным интетратором и без него) являются устойчивыми независимо от отклонения уровней сигнала и шума от их номинальных значений. Показать, что это неверно для систем третьего порядка.

5.5. Точный анализ нелинейной модели системы ФАПЧ первого порядка приводит к распределению фазовой ошибки, называемому распределением *Тихонова*:

$$\rho(\Phi)=\exp\left[R_L\, g(\Phi)\right]\Big/\int\limits_{-\pi}^{\pi}\exp\left[R_L\, g(\Phi)\right]d\Phi;\quad |\Phi|\leqslant\pi,$$

где $g(\Phi)=\int\limits_{-\pi}^{\Phi}\rho_{xz}(T\eta/2\pi)\,d\eta$, а $\rho_{xz}(\tau)$ определяется в (5.104), и где $R_L=4A/N_0K$; A^2 — мощность принимаемого сигнала; N_0 — спектральная плотность шума и K — постоянное усиление ГУН. (Этот результат справедлив, когда фаза принимаемого сигнала постоянна, шум является белым и гауссовским и фазовая ошибка берется по модулю 2π.) Показать, что распределение фазовой ошибки в действительности является приближенно гауссовским для достаточно больших значений R_L с дисперсией σ_Φ^2 в соответствии с тем, что предсказывает линейная модель [с эффективной амплитудой сигнала, задаваемой ф-лой (5.109)]. Показать далее, что если $\rho_{xz}(\tau)$ — нечетная функция τ и если существуют ее первые три производные, то гауссовское приближение справедливо для всех R_L, для которых

$$\sigma_\Phi^2\ll\frac{48\pi^2}{T^2}\left|\frac{\rho'_{xz}(0)}{\rho'''_{xz}(0)}\right|.$$

5.6. Сигнал $y(t)=\sqrt{2}A\sin(\omega_c t+\theta)+n(t)$, где $n(t)$ — белый гауссовский шум, проходит через полосовой фильтр с шириной полосы шума B_1 и центральной частотой ω_c. Выход фильтра, в свою очередь, проходит через устройство с нечетной ν-характеристикой [т. е. устройство, которое превращает вход $x(t)$ в выход $|x(t)|^{\nu}\mathrm{sgn}(x(t))$], за которым следует второй полосовой фильтр с шириной полосы шума B_2 и центральной частотой ω_c. Показать, что если $B_2\ll B_1\ll\omega_c$ и отношение сигнал/шум на входе достаточно велико, то отношение сигнал/шум на выходе обратно пропорционально $1+\nu^2$ и, следовательно, максимизируется при $\nu=0$. (Здесь отношение сигнал/шум определяется как отношение среднеквадратического значения сигнала, которое наблюдалось бы в отсутствие шума, к разности между этим сигналом и в действительности наблюдаемым сигналом.) Показать, что точность, с которой этот сигнал может быть отслежен системой ФАПЧ в этих условиях в противоположность вышесказанному, не зависит от ν. (*Указание:* выразить вход устройства с ν-характеристикой в виде $B\sin(\omega_c t+\Psi)$ и найти синфазную и квадратурную компоненты основного сигнала на его выходе.) Как это сказывается (при рассмотрении системы ФАПЧ) на увеличении на 3 дБ отношения сигнал/шум, которое получается (когда это отношение велико) при пропускании такого сигнала через полосовой ограничитель? (См. с. 135).

ЧАСТЬ II

СИНХРОНИЗАЦИЯ

Глава 6

СИНХРОНИЗАЦИЯ ПО ОТДЕЛЬНОМУ КАНАЛУ

6.1. Введение

Эта и две последующие главы посвящены методам установления синхронизации, необходимой для эффективной работы систем связи того типа, который был описан в гл. 3 и 4. Вероятно, наиболее простым и самым прямым способом дать такую информацию является использование отдельного канала (или каналов) связи, отведенного единственно для целей синхронизации. Некоторые стороны этого подхода исследуются в этой главе.

Как обсуждалось в гл. 1, первый шаг процедуры синхронизации состоит обычно в том, чтобы связать отсчеты времени приемника и передатчика и посредством этого установить общий отсчет времени (несущую) для всей системы. Вторым шагом является увеличение интервала времени, в котором отсутствует неоднозначность, до заранее выбранного интервала в T_0 секунд.

Для того чтобы привязать отсчет времени приемника к отсчету времени передатчика, нужно передавать периодический сигнал вместе с сообщением и отслеживать его фазу в приемнике. Обычно сигнал времени одновременно служит несущей или поднесущей и поэтому часто синусоидален. Однако независимо от того, какой периодический сигнал используется, оптимальный приемник, по существу, является системой ФАПЧ, как мы пытались показать в предыдущей главе. Последующие два параграфа исследуют связь между сигналом времени и достижимой точностью отслеживания.

6.2. Синусоидальные сигналы времени

Если сигнал времени выбирается в виде синусоиды, то приемник, по-видимому, должен содержать систему ФАПЧ, использующую опорную синусоиду, как обсуждалось в гл. 5. В этих условиях единственное, что осталось определить в сигнале и структуре приемника, — частота сигнала и структура фильтра ФАПЧ. Более того, выбор их нельзя произвести независимо. Как было показано в гл. 5, оптимальный фильтр ФАПЧ полностью определяется отношением сигнал/шум и статистическими свойствами фазы или предсказываемыми фазовыми переходными процессами. Отношение сигнал/шум определяется внешними ограничениями. Аналогично, фазовые характеристики определены по заданным стабильностям генераторов передатчика и приемника и по их относительному уходу. Единственная неопределенность в этих характеристиках связана с величиной, которая, как будет сейчас показано, является функцией частоты генератора. Таким образом, фактически единственным, что остается выбрать, является частота.

Если дисперсия фазовой ошибки равна $\sigma^2{}_0$, рад^2, а частота сигнала равна $\omega_0=2\pi/T_0$ рад/с, то дисперсия ошибки отслеживания, выраженная в с^2, равна $\sigma_{\tau}=\sigma^2{}_0/\omega^2{}_0$. Очевидно, ошибка синхронизации могла бы быть снижена простым увеличением частоты сигнала времени от ω_0 рад/с до, например, $\omega>\omega_0$ рад/с. Но это лишь одна сторона вопроса, так как характеристика фильтра и, следовательно, дисперсия фазовой ошибки $\sigma^2{}_0$ также являются функциями ω. А именно, фильтр ФАПЧ выбирается в результате компромисса между необходимостью уменьшить влияние случайно изменяющейся или переходной фазы сигнала и влияние аддитивного шума. Чтобы минимизировать ошибку отслеживания, обусловленную аддитивным шумом, ширина полосы системы должна быть сделана как можно меньшей; чтобы минимизировать переходную ошибку, ширина полосы должна быть сделана как можно большей. Так как величина переходной ошибки, по-видимому, прямо пропорциональна частоте сигнала, то чем выше частота, тем больше требуемая ширина полосы системы. Таким образом, если фиксированы мощность сигнала и спектральная плотность шума, можно ожидать, что ошибка отслеживания фазы увеличивается при увеличении номинальной частоты системы ФАПЧ.

Однако это увеличение дисперсии ошибки самое большее прямо пропорционально увеличению частоты. На самом деле присутствие аддитивного шума и возникающая вследствие этого необходимость компромисса между этими двумя источниками ошибок обычно приводят к увеличению ширины полосы оптимальной цепи и, следовательно, дисперсии фазовой ошибки, но не пропорционально частоте сигнала. Поэтому обычно дисперсия фазовой ошибки может быть записана в виде $\sigma^2{}_0(\omega/\omega_0)^r$ рад^2, где r — некоторое число из интервала $(0,1)$ и $\sigma^2_\tau=(\sigma^2{}_0/\omega^r{}_0)(1/\omega^{2-r})$ с^2. Таким образом σ_τ обратно пропоциональна $\omega^{1-r/2}$ и уменьшается с ростом ω.

Конечно, ω не может быть сделана произвольно большой. Корень квадратный из среднеквадратического значения фазовой ошибки должен быть малым по сравнению с $\pi/2$ рад, если система ФАПЧ должна оставаться в режиме захвата в течение большого периода времени, т. е. условие

$$\sigma_0(\omega/\omega_0)^{r/2}=\pi/2k \tag{6.1}$$

должно выполняться для некоторой достаточно большой постоянной k. [Значение k должно быть порядка 3 или выше, если вероятность потери синхронизации должна быть достаточно малой (ср. с § 5.8)]. В соответствии с этим максимальная приемлемая частота сигнала

$$\omega = \omega_0 \left(\frac{\pi}{2k\,\sigma_0} \right)^{2/r} \tag{6.2}$$

и дисперсия (в рад^2) фазовой ошибки системы ФАПЧ, работающей на этой частоте,

$$\sigma_\Phi^2 = \sigma_\tau^2 \omega_0^2 = \left(\frac{4k^2}{\pi^2} \right)^{(2/r)-1} \sigma_0^{4/r} . \tag{6.3}$$

Здесь для целей сравнения дисперсия выражена через первоначальный период $T_0 = 2\pi/\omega_0$ (т. е. 2π рад соответствуют T_0 секунд). Дисперсия фазовой ошибки системы ФАПЧ, использующей максимальную приемлемую частоту, пропорциональна $(2/r)$-степени дисперсии $\sigma^2{}_0$ системы ФАПЧ, работающей на частоте ω_0, при условии, конечно, что эта дисперсия мала по сравнению с единицей.

Для примера рассмотрим систему второго порядка, предназначенную для отслеживания скачка частоты величины $\Delta\omega/2\pi$. В соответствии с изложенным в § 5.6 имеем

$$\sigma_0^2 = \frac{N_c B_L}{A_0^2} = \frac{3}{4\,(2)^{1/4}} \left(\frac{N_0}{A_0^2} \right)^{3/4} (\lambda \Delta\omega)^{1/2} .$$

Так как величина скачка частоты по предположению прямо пропорциональна частоте, то r в этом случае равно $1/2$[1]). (Обычно r равно обратной величине порядка системы; см. § 5.6). Отсюда

$$\sigma_\Phi^2 = \left(\frac{2k}{\pi} \right)^6 \sigma_0^8 = \left(\frac{2k}{\pi} \right)^6 \left(\frac{N_0 B_L}{A_0^2} \right)^4 , \tag{6.4}$$

что обеспечивает значительное улучшение, когда $N_0 B_L / A^2{}_0$ мало по сравнению с единицей.

6.3. Несинусоидальные сигналы времени

Как было изложено в § 5.8, характеристика системы ФАПЧ при отслеживании сигнала $y(t) = Ax(t) + n(t)$ с помощью местного сигнала $z(t)$ (см. рис. 5.2) совпадает с характеристикой той же системы в случае, когда $x(t)$ и $z(t)$ — синусоиды, для которых корень квадратный из среднеквадратического значения амплитуды принимаемого сигнала

$$A_e = \frac{AT_0}{2\pi} \left| \rho'_{xz}(0) \right| , \tag{6.5}$$

где T_0 — период сигнала.

---

[1] Параметр λ не зависит от частоты; он просто представляет собой относительный вес, приписываемый шумовой и переходной ошибкам. Чтобы проверить это, заметим, что если λ постоянна, то $\sigma^2{}_n$ и $e^2{}_T$ зависят от $\Delta\omega$ одинаково (ср. с § 5.6). (*Прим. авт.*).

Приведем пример характеристики отслеживания, которую можно получить при использовании несинусоидальных сигналов; пусть $x(t)$ — периодический импульсный сигнал с длительностью импульса ΔT и периодом повторения T_0. Так как форма импульса для дальнейшего имеет второстепенное значение (ср. с задачей 6.2), то для удобства предположим, что она прямоугольна:

$$x(t)=\begin{cases}\sqrt{T_0/\Delta T} & \text{при } -\dfrac{\Delta T}{2}<t<\dfrac{\Delta T}{2} \text{ по модулю } T_0;\\ 0 & \text{в остальных случаях.}\end{cases} \tag{6.6}$$

Пусть местный сигнал $z(t)$ определяется равенством

$$z(t)=\begin{cases}\sqrt{T_0/2\Delta t} & \text{при } -\dfrac{\Delta T+\Delta t}{2}<t<-\dfrac{\Delta T-\Delta t}{2} \text{ по модулю } T_0;\\ -\sqrt{T_0/2\Delta t} & \text{при } \dfrac{\Delta T-\Delta t}{2}<t<\dfrac{\Delta T+\Delta t}{2} \text{ по модулю } T_0;\\ 0 & \text{в остальных случаях,}\end{cases} \tag{6.7}$$

где $\Delta t \leqslant \Delta T$. Эти функции изображены на рис. 6.1 вместе с их взаимокорреляционными функциями $\rho_{xz}(\tau)$, которые в области, представляющей основной интерес, имеют вид

$$\rho_{xz}(\tau)=-\tau\sqrt{2/\Delta T\,\Delta t};\quad |\tau|<\Delta t/2. \tag{6.8}$$

Производная корреляционной функции $\rho_{xz}(\tau)$ в области $|\tau|<\Delta t/2$ обратно пропорциональна $(\Delta t)^{1/2}$. Это могло бы означать, что, устремляя Δt к нулю, можно минимизировать ошибки отслеживания. В самом деле, если $\Delta t\to 0$, $z(t)\to x'(t)$, т. е. стремится к местному сигналу, оптимальному с точки зрения максимума $\rho'_{xz}(0)$. Очевидно, однако, что Δt нельзя сделать сколь угодно малым, так как максимальная величина $\rho_{xz}(\tau)$ *прямо* пропорциональна $(\Delta t)^{1/2}$. Чтобы определить наилучшее значение Δt, следует принять во внимание, что оптимальная ширина полосы системы ФАПЧ B_e является функцией эффективной амплитуды сигнала A_e [равенство (6.5)]. А именно: $B_e=B_L(A_e/A)^r$, где B_L — ширина полосы оптимальной системы ФАПЧ, предназначенной для отслеживания синусоиды с амплитудой A, и r зависит от порядка системы. (Опять r обычно равно обратной величине порядка системы.) Поэтому среднеквадратическая фазовая ошибка,

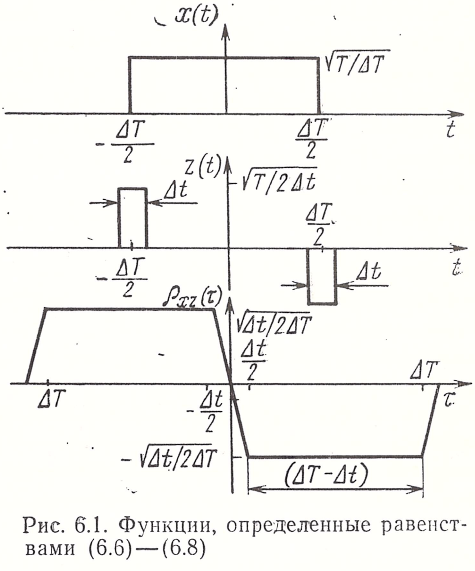


Рис. 6.1. Функции, определенные равенствами (6.6)—(6.8)

обусловленная аддитивным шумом, в случае когда $x(t)$ и $z(t)$ заданы равенствами (6.6)—(6.8),

$$\sigma_\Phi^2=\frac{N_0B_e}{A_e^2}=\sigma_0^2\left(2\pi^2\frac{\Delta T}{T_0}\,\frac{\Delta t}{T_0}\right)^{1-(r/2)}, \tag{6.9}$$

где $\sigma_0^2=N_0B_L/A^2$ представляет собой ошибку отслеживания, если сигнал является синусоидальным с периодом T_0.

Чтобы равенство (6.9) было справедливо, система ФАПЧ с большой вероятностью должна работать в линейной области $|\tau|\leqslant\Delta t/2$. Для того чтобы быть уверенным, что этот случай имеет место, и избежать трудностей, связанных со стремлением Δt к нулю, введем дополнительное ограничение в виде

$$\sigma_\Phi=\frac{\pi}{k}\,\frac{\Delta t}{T_0} \tag{6.10}$$

для некоторого достаточно большого k (ср. с § 6.2). Объединяя равенства (6.9) и (6.10) и разрешая их относительно Δt, находим, что

$$\frac{\Delta t}{T_0}=\left(2\pi^2\frac{\Delta T}{T_0}\right)^{(2-r)/(2+r)}\left(\frac{k\sigma_0}{\pi}\right)^{4/(2+r)};$$

используя это значение Δt, получаем

$$\sigma_\Phi^2=(2k\pi\Delta T/T_0)^{2[(2-r)/(2+r)]}\,\sigma_0^{8/(2+r)}. \tag{6.11}$$

Среднеквадратическая ошибка при отслеживании прямоугольного импульса, например, системой второго порядка пропорциональна $(N_0B_L/A^2)^{8/5}$, когда местный сигнал определяется равенствами (6.6)—(6.8) и Δt выбирается в соответствии с предыдущим обсуждением. Это указывает на потенциальное улучшение по сравнению с ошибкой отслеживания синусоиды того же самого периода, хотя это улучшение значительно менее эффективно, чем то, которое (как было показано) достигается при использовании высокочастотных синусоид (§ 6.2). Рассмотренная схема имеет то преимущество, что в исходном интервале в T_0 секунд она не имеет многократных точек, где происходит захват.

До сих пор параметр ΔT (длительность принимаемого импульса) подразумевался фиксированным и постоянным. Если это не так, то его тоже можно оптимизировать почти таким же методом, как параметр Δt. Объединяя опять равенства (6.9) и (6.10) и решая их относительно Δt, получим

$$\frac{\Delta T}{T_0}=\frac{2^{(2-r)/2r}\,k^{2/r}\,\sigma_0^{2/r}}{\pi\,(\Delta t/\Delta T)^{(2+r)/2r}},$$

где отношение $\Delta t/\Delta T$ временно считается постоянным. Подставляя это соотношение в (6.9) или в (6.10), находим

$$\sigma_\Phi^2=\left(\frac{2k^2}{\Delta t/\Delta T}\right)^{(2/r)-1}\sigma_0^{4/r}. \tag{6.12}$$

Теперь ошибка отслеживания обратно пропорциональна Δt. Так как равенства (6.6) — (6.8) справедливы только для $\Delta t \leqslant \Delta T$ (и, очевидно, выбор $\Delta t > \Delta T$ не дает преимущества), то оптимальной величиной для Δt здесь является ΔT. Таким образом, приходим к следующим выводам. Если принимаемый импульс достаточно широк, выгодно уменьшить по возможности длительность местного сигнала, но так, чтобы она согласовалась с требуемой вероятностью потери синхронизации. Однако если можно оптимизировать длительность импульса передаваемого сигнала, то ее нужно выбрать по возможности малой при том же самом ограничении относительно потерь синхронизации. Если эта возможность существует, то никаких других преимуществ нельзя получить, уменьшая длительность импульса местного сигнала. В то время как при оптимизации длительности местного импульса [равенство (6.11)] можно достичь лишь довольно скромного улучшения, преимущества, которые могут быть получены при оптимальном выборе длительности передаваемого импульса, по существу, будут такими же, как при оптимизации частоты передаваемой синусоиды [ср. с равенствами (6.12) и (6.3)].

Иногда в качестве сигнала времени используется не синусоида, а прямоугольные импульсы, причем местный сигнал $z(t)$ может быть либо синусоидой, либо другой последовательностью прямоугольных импульсов. В этом случае легко выбрать оптимальную частоту следования прямоугольных импульсов, используя метод, рассмотренный в § 6.2. Если $z(t)$ синусоида, имеем

$$\rho_{xz}(\tau) = \frac{2\sqrt{2}}{\pi} \sin \frac{2\pi\tau}{T_0},$$

и эффективная амплитуда сигнала равна $(2\sqrt{2}/\pi)A$, что приводит к небольшому ухудшению по сравнению со случаем, когда передаваемый сигнал также является синусоидой. Аналогично если $z(t)$ — последовательность прямоугольных импульсов, то эффективная амплитуда сигнала уменьшается еще больше, до величины $2A/\pi$.

Оптимальной корреляционной функцией $\rho_{xz}(\tau)$, очевидно, должна была бы быть прямоугольная функция с единичной амплитудой, имеющая бесконечную производную в точке $\tau = 0$ и абсолютное значение, равное единице для всех $\tau \neq 0$ по модулю T_0. К сожалению, взаимокорреляционная функция любых двух сигналов конечной энергии не может иметь такого вида. Точное описание «оптимальной» реализуемой корреляционной функции дать нелегко, помимо прочего, из-за того, что трудно установить, какие отклонения от идеальной прямоугольной корреляционной функции наименее нежелательны.

Если рассматривать лишь абсолютное значение производной $|\rho'_{xz}(0)|$ корреляционной функции в точке $\tau = 0$, то его можно было бы сделать сколь угодно большим с помощью любого из методов, описанных здесь и в предыдущем параграфе. Это достигается за счет сужения линейной области и введения многократных точек захвата или, в случае узкого импульса, за счет потенциального увеличения времени входа в синхронизм из-за больших интервалов τ, в которых $\rho_{xz}(\tau)$ и, следовательно, сигнал ошибки равны нулю. Другой подход поэтому мог бы состоять в попытке максимизации величины $|\rho'_{xz}(0)|$ при условии, накладываемом на всю функцию $\rho_{xz}(\tau)$: например, при условии, что $\rho_{xz}(\tau)$ монотонно неубывающая функция τ в области $|\tau| \leqslant T_0/4$.

Это условие удовлетворялось бы, например, для класса сигналов, рассмотренных в этом параграфе, если бы ΔT в ф-ле (6.5) равнялось $T_0/2$. Как было указано выше, длительность импульса местного сигнала Δt могла бы в этом случае быть минимизирована (для того, чтобы максимизировать $|\rho'_{xz}(0)|$). Сравнительно скромное улучшение, получаемое при этом по сравнению с использованием, например, синусоиды с частотой $f=1/T_0$, является следствием того, что нужно платить за глобальные, а не за локальные ограничения на корреляционную функцию $\rho_{xz}(\tau)$. Следовательно, для того чтобы максимизировать эффективность использования имеющейся мощности, часто необходимо использовать высокочастотную синхронизацию и устранять возникающие в результате этого неопределенности другими методами. В частности, это верно в тех случаях, когда ограничения на пиковую мощность, или ширину полосы, или время входа в синхронизм снижают эффективность метода сужения импульса.

6.4. Поиск метки

Если в целях уменьшения мощности, требуемой для синхронизации, период ΔT сигнала времени выбирается меньше, чем основной интервал неоднозначности длиной T_0 секунд, то процедура синхронизации не заканчивается входом в синхронизм. При этом остаются $N\Delta\ T_0/\Delta T$ точек или *меток* в каждом интервале T_0, каждая из которых может представлять правильную опорную точку синхронизации. Определение среди них правильной метки можно осуществить, передавая второй сигнал синхронизации $x(t)$, период которого равен минимальному периоду T_0, и определяя фазу этого сигнала в приемнике.

С первого взгляда этот подход, казалось бы, не дает никакого преимущества перед использованием сигнала с периодом T_0 для самого отсчета времени. Однако наличие опорного отсчета времени необходимо для достижения требуемой точности отслеживания. Цель второго сигнала состоит лишь в разрешении остающейся N-кратной неоднозначности во времени. Как следствие, мощность этого сигнала значительно меньше той, которая была бы необходима для него в случае, если он был бы также сигналом времени. Поэтому полная требуемая мощность может быть значительно снижена при использовании двух сигналов вместо одного.

Задача приемника теперь состоит в определении того, какой из сигналов $Ax_\nu(t)=Ax(t-\nu\Delta T)$, $\nu=0,\ 1,\ \ldots,\ N-1$ фактически был принят на фоне обычного аддитивного белого гауссовского шума.

Такая задача эквивалентна задачам приема, рассмотренным в гл. 4. Решение по максимуму правдоподобия¹) состоит в формировании корреляций

$$z_\nu = \sum_{j=0}^{M-1} \int_{jT_0}^{(j+1)T_0} y(t)\, x(t-\nu\Delta T)\, dt \triangleq \sum_{j=0}^{M-1} z_{\nu j}; \quad \nu=0, 1, \ldots, N-1 \qquad (6.13)$$

и выборе наибольшей из них. Период наблюдения MT_0 здесь, в противоположность ситуации, рассмотренной в гл. 4, не обязательно ограничивается длительностью принимаемого сигнала, который также может передаваться неопределенно долго. Более того, если местный сигнал $x(t)$ синхронизирован по времени с помощью восстановленного отсчета времени, то часто неприятный случайный уход разности фаз местного и принимаемого сигналов, по существу, не будет возникать. Тем не менее обычно хотят принять решение относительно метки по возможности быстрее. В соответствии с этим цель параграфа — оценить минимальное значение M, такое, для которого решение может быть принято с заранее установленной, достаточно малой вероятностью ошибки.

Эта ситуация имеет еще одно отличие от рассмотренной в гл. 4, а именно: ограничения на сложность устройства часто делают невозможной одновременную обработку наблюдаемых, относящихся к каждой из меток. В этом случае можно использовать процедуру поиска. К задаче, рассматриваемой в этом параграфе, применимы как алгоритм с фиксированным объемом выборки, так и алгоритм последовательного поиска из гл. 2.

Одновременное наблюдение. Так как шум является белым и гауссовским, переменные $z_{\nu j}$ *(решающие переменные)*²) распределены по Гауссу со средними

$$\eta_\nu(\mu) \triangleq E(z_{\nu j} \mid \mu) = \int_{jT_0}^{(j+1)T_0} A x_\mu(t)\, x_\nu(t)\, dt \triangleq A T_0 \rho_i \triangleq \eta_i, \quad \nu=0, 1 \ldots, \qquad (6.14)$$

и ковариациями

$$\sigma^2_{\mu\nu} \triangleq E(z_{\mu j} z_{\nu j}) - E(z_{\mu j}) E(z_{\nu j}) =$$

$$= \frac{N_0}{2} \int_{jT_0}^{(j+1)T_0} x_\mu(t)\, x_\nu(t)\, dt = \frac{N_0}{2} T_0 \rho_i \triangleq \sigma^2 \rho_i, \qquad (6.15)$$

где μ означает правильную метку, а $i=\mu-\nu$ по модулю N. (Без

---

¹) Повсюду в этой главе будет предполагаться, что априорная вероятность $P(\nu)$ того, что ν-метка является правильной, не зависит от ν; $P(\nu)=1/N$, $\nu=0, 1, \ldots, N-1$. Таким образом, термины «синхронизация максимального правдоподобия» и «синхронизация по максимуму апостериорной вероятности» могут быть использованы на равных правах. *(Прим. авт.)*.

²) Термин «решающие переменные» часто используется для обозначения статистик, на которых фактически основывается решение. *(Прим. авт.)*.

потери общности можно считать, что $(1/T_0)\int\limits_0^{T_0} x_\mu^2(t)dt=1$, так что $|\rho_i|\leqslant 1$).

Ситуация здесь совпадает с той, которая была рассмотрена в § 4.2. В частности, здесь непосредственно применимы границы (4.20). Вероятность ошибочного решения ограничена следующим образом:

$$\frac{e^{-r^2/2}}{(2\pi)^{1/2} r}\left(1-\frac{1}{r^2}\right)\leqslant P_e\leqslant \frac{e^{-[(r^2/2)-\log_e (N-1)]}}{(2\pi)^{1/2} r}, \qquad (6.16)$$

где $r^2 \underline{\Delta} \min\limits_{\substack{\mu,\nu\\ \mu\neq\nu}} \dfrac{E^2(z_\nu - z_\mu|\nu)}{\mathrm{var}\,(z_\nu - z_\mu|\nu)} = MR(1-\rho)$; $\rho \underline{\Delta} \max\limits_{i\neq 0}\rho_i$ и $R=A^2T_0/N_0$.

Если вероятность P_e должна быть малой, то r^2 должно быть велико по сравнению с единицей. Таким образом, логарифмируя неравенство (6.16), получим

$$2\log_e(1/P_e)\leqslant r^2\leqslant 2\log_e(1/P_e)+2\log_e(N-1) \qquad (6.17)$$

или, в более удобной форме,

$$r^2=2K_N\log_e(1/P_e), \qquad (6.18)$$

где $1\leqslant K_N\leqslant 1+[\log_e(N-1)/\log_e(1/P_e)]$. Члены порядка $\log_e r$ были опущены, так как они малы по сравнению с r^2. Обычно вероятность P_e мала по сравнению с $1/N$, так что обе границы для r^2 будут довольно близкими.

Как следствие, из ф-л (6.17), (6.18) получаем

$$M=[2K_N\log_e(1/P_e)]/R(1-\rho), \qquad (6.19)$$

и требуемое время наблюдения равно MT_0 секунд. Если $\rho_i=\rho$ для всех $i\neq 0$, то точное выражение для вероятности ошибки, полученное в § 4.2, разумеется, в равной мере применимо и здесь. Чтобы применить эти результаты к настоящей задаче, нужно лишь подставить величину $(1-\rho)MR/\log_2 N$ вместо величины R_b, указанной на рисунке 4. 2.

Поиск с фиксированным объемом выборки. Чтобы применить алгоритм поиска, описанный в § 2.5, в рассматриваемой здесь ситуации, будем проверять на ν-м этапе поиска нулевую гипотезу H_ν (что меткой принятого сигнала является ν-я метка по модулю N) относительно некоторой альтернативной гипотезы $\overline{H}_\nu$. Наблюдаемыми будут статистики z_ν, определяемые равенством (6.13) [1]).

Хотя альтернативная гипотеза $\overline{H}_\nu$ очевидно, является сложной, разумно и целесообразно заменить ее какой-либо простой гипотезой H_μ с любым $\mu \neq \nu$. Логарифм отношения правдоподобия здесь имеет вид

---

[1]) Эти статистики, очевидно, не являются достаточными; чтобы принять оптимальное решение, нужны все статистики z_1, z_2, ..., z_N. Но цель поиска в первую очередь состоит в том, чтобы избежать необходимости одновременной обработки всех этих величин. *(Прим. авт.)*.

$$\log_e \frac{p(z_\nu|\nu)}{p(z_\nu|\mu)} = \log_e \Lambda_{\nu\mu} = \frac{\eta_0(1-\rho_i)}{\sigma^2} z_\nu - \frac{M\eta_0^2(1-\rho_i^2)}{2\sigma^2}, \tag{6.20}$$

где η_0, σ^2 и ρ_i определены равенствами (6.14), (6.15). Если имеются лишь две возможные метки, наиболее мощным тестом гипотезы H_ν при любом уровне значимости α_ν будет принятие ее, если решающая переменная z_ν превышает некоторый порог a_ν и отвержение ее в остальных случаях. Но так как $\rho_i < 1$ для всех $i \neq 0$, то область принятия H_ν при любом заданном α_ν не зависит от μ. Тест (6.20) гипотезы H_ν поэтому является равномерно наиболее мощным относительно всех альтернативных гипотез H_μ. Независимо от альтернативной гипотезы гипотеза H_ν принимается, если z_ν превышает порог a_ν и отвергается в остальных случаях.

По причинам, указанным в § 2.5, ограничимся рассмотрением наиболее простых алгоритмов поиска с фиксированным объемом выборки. Каждая гипотеза будет проверяться при одном и том же уровне и будет проверяться достаточно долго, чтобы гарантировать малую вероятность ошибочного решения. Поэтому порог a_ν будет поддерживаться постоянным независимо от ν и будет выбираться так, чтобы были малыми вероятности ошибок обоих родов. По предположению ошибка возникает и в том случае, если решение не будут вынесено к моменту, когда все N состояний были проверены.

Чтобы оценить число наблюдаемых, необходимых для завершения поиска, обозначим через α вероятность ошибочно отвергнуть гипотезу H_ν, а через $\beta_\nu(\mu)$ — вероятность ее принять, когда в действительности правильной является μ-я метка. Далее пусть $a \triangleq M\eta_0[\rho + \gamma(1-\rho)]$ будет порогом при решении, где $\rho \triangleq \max\limits_{i \neq 0} |\rho_i|$; величина η_0 была определена выше. (Хотя величина γ не была задана, это не накладывает какого-либо ограничения на a. Однако, если α и $\beta_\nu(\mu)$ должны быть малыми, γ должна, очевидно, лежать в интервале $0 \leqslant \gamma \leqslant 1$). Тогда

$$\alpha_\nu = \alpha = \Pr\{z_\nu < a | \nu\} = \frac{1}{2}\{1 - \operatorname{erf}[(1-\gamma) r]\}, \tag{6.21}$$

где $r^2 = M(1-\rho)^2 \eta^2{}_0 / 2\sigma^2$. Аналогично

$$\beta_\nu(\mu) = \Pr\{z_\nu > a \mid \mu\} \leqslant \frac{1}{2}[1 - \operatorname{erf} \gamma r] \triangleq \beta, \tag{6.22}$$

где равенство выполняется, если $\rho_i = \rho$ для всех $i \neq 0$.

Если бы ρ_i были одинаковы для всех $i \neq 0$, то при условиях, указанных выше (ср. с § 2.5),

$$P_e \approx \alpha + \frac{N-1}{2} \beta. \tag{6.23}$$

Как α, так и β являются функциями γ, поэтому можно определить значение γ, которое минимизирует P_e. Когда применимо приближение (6.23), оптимальное значение γ определяется уравнением $\frac{d\alpha}{d\gamma}+\frac{N-1}{2}\frac{d\beta}{d\gamma}=0$, которое удовлетворяется, если

$$0\leqslant\gamma=\frac{1}{2}\left(1+\frac{1}{r^2}\log_e\frac{N-1}{2}\right)\leqslant 1. \tag{6.24}$$

Подставляя это значение γ в (6.23) и используя асимптотическое разложение интеграла вероятности, получим

$$P_e=\frac{2\exp\left\{-\left(1-\frac{\log_e\frac{N-1}{2}}{r^2}\right)^2\frac{r^2}{4}\right\}}{\sqrt{\pi}\,r\left[1-\left(\frac{\log_e\frac{N-1}{2}}{r^2}\right)^2\right]}\left[1+0\left(\frac{1}{r^2}\right)\right]\triangleq P_0(N). \tag{6.25}$$

Вновь, в силу того что r^2 должно быть большим, если P_e должна быть малой, находим, логарифмируя обе части (6.25) и пренебрегая членами порядка $\log_e r$, что

$$r^2=4K'_N\log_e(1/P_e), \tag{6.26}$$

где

$$K'_N=\frac{1}{2}+\frac{\log_e[(N-1)/2]}{4\log_e(1/P_e)}+\frac{1}{2}\left(1+\frac{\log_e[(N-1)/2]}{\log_e(1/P_e)}\right)^{1/2}.$$

Если ρ_i не обязательно равны, вероятность P_e можно все же оценить следующим образом. Очевидно, вместо равенства (6.23) справедливо неравенство

$$P_e\leqslant\alpha+\frac{N-1}{2}\beta, \tag{6.27}$$

где β определено ф-лами (6.21) и (6.22). Более того, так как с вероятностью β ошибочно принимается, по меньшей мере, одна метка и так как с вероятностью 1/2 она будет проверена ранее правильной метки, то

$$P_e\geqslant\frac{1}{2}(\beta+\alpha(1-\beta))+\frac{1}{2}\alpha\approx\alpha+\frac{1}{2}\beta. \tag{6.28}$$

Используя для решения оптимальные пороги, определяемые ф-лой (6.24), получаем следующие верхнюю и нижнюю границы для P_e:

$$P_0(2)\leqslant P_e\leqslant P_0(N) \tag{6.29}$$

[см. (6.25)] и, следовательно,

$$r^2=4K''_N\log_e(1/P_e), \tag{6.30}$$

где $K'_2\leqslant K''_N\leqslant K'_N$.

Математическое ожидание времени поиска равно $E(\nu)MT_0\triangleq\triangleq M_TT_0$, где ν — число меток, проверенных до завершения поиска.

Когда $P_e \ll 1$, из равенства (2.35) следует, что $E(\nu) \approx (N+1)/2$, а из равенства (6.30) — что

$$\overline{M}_T \approx \frac{2(N+1)\, K''_N \log_e (1/P_e)}{R\,(1-\rho)^2} \qquad (6.31)$$

где R было определено ранее.

Задержанное решение. Интересной модификацией метода с фиксированным объемом выборки является такой, при котором принимается *задержанное решение* относительно правильной метки. То есть решение задерживается до тех пор, пока не будут обработаны все наблюдаемые z_ν, $\nu = 0, 1, 2, \ldots, N-1$, даже если корреляции, которые дают эти наблюдаемые, вычисляются поочередно. Несомненно, что наиболее простым правилом решения является выбор в качестве правильной метки той, для которой значение ν максимизирует z_ν. (Очевидно, это решение является подоптимальным; сейчас рассматривается оптимальное задержанное решение.).

Вероятность ошибки при вынесении такого решения удовлетворяет тем же границам [ср. с ф-лой (6.16)], что и вероятность ошибки при параллельном решении. Единственное отличие состоит в том, что вычисление статистик z_ν производится не одновременно. Таким образом, $\sigma^2_{\nu\mu} = 0$; $\mu \neq \nu$ и член r^2 в (6.16) следует определить так, как в равенствах (6.21) и (6.22). Поэтому здесь равенство (6.19) приобретает вид

$$M_T = \frac{2NK_N \log_e (1/P_e)}{R\,(1-\rho)^2}\,. \qquad (6.32)$$

Интересно сравнить равенства (6.31) и (6.32), особенно, когда N велико и $P_e \ll 1/N$, что является типичным. В этом случае все K_N, K'_2, K'_N и, следовательно, K''_N приближенно равны единице, и оба времени поиска, по существу, совпадают. Испытываются ли все метки поочередно и принимается (подоптимальное) задержанное решение, или используется алгоритм поиска с фиксированным объемом выборки — это лишь незначительно изменяет характеристику. Наиболее важным отличием является то, что время поиска в последнем случае является случайной величиной и с равной вероятностью принимает любое значение от $[2/(N+1)]\overline{M}_T T_0$ до $[2N/(N+1)]\overline{M}_T T_0$.

Для того чтобы придать этим результатам более конкретную форму и продемонстрировать один из недостатков алгоритма поочередного поиска с фиксированным объемом выборки, допустим, что сигнал синхронизации имеет вид

$$x(t) = \begin{cases} \sqrt{n}, & 0 < t < \dfrac{T_0}{n}\,; \\[2ex] 0, & \dfrac{T_0}{n} < t < T_0 \end{cases} \qquad (6.33)$$

для некоторого целого n; $2 \leqslant n \leqslant N$; максимальная допустимая неоднозначность во времени равна T_0/N секунд. Тогда

$$\rho\left(\frac{\nu T_0}{N}\right) \triangleq \rho_\nu = \begin{cases} 1 - \left|\dfrac{\nu n}{N}\right| & \text{при } |\nu| \leqslant \dfrac{N}{n}; \\ 0 & \text{в остальных случаях.} \end{cases}$$

и $\rho = \max\limits_{\neq} \rho_\nu = 1 - (n/N)$. Подставляя эту величину в ф-лы (6.19) и (6.32) [или в (6.31)], получаем

$$M_T = 2NK_N \log_e (1/P_e)/nR \tag{6.34}$$

для одновременной обработки наблюдаемых и

$$M_T = 2N^3K_N \log_e (1/P_e)/n^2R \tag{6.35}$$

для поочередной обработки. Когда N велико, ограничение, состоящее в необходимости поочередной обработки, может привести к значительному ухудшению характеристики[1]). Можно было бы надеяться, что этот результат можно улучшить, когда n мало по сравнению с N, но поочередный поиск в том виде, как он представлен здесь, очевидно, не является эффективным в этом случае. Все (независимые) статистики z_ν [см. (6.13)] должны быть обработаны (по крайней мере, методом задержанного решения). Однако лишь одна из них, наибольшая, влияет на решение. То, что z_1 и z_{N-1} должны быть почти столь же велики, как и z_0 (когда $\nu=0$ представляет собой правильную метку), и то, что $z_{N/2}$ должна быть намного меньше, чем каждая из этих величин, не принимается в расчет при решении.

В действительности при заданных статистиках оптимальное решение (максимального правдоподобия) состоит в принятии метки, максимизирующей функцию правдоподобия $p(z_0, z_1, \ldots, z_{N-1}|\nu)$. Так как статистики z независимы, когда наблюдения производятся поочередно, то

$$p(z_0, z_1, \ldots, z_{N-1}|\nu) = \frac{1}{(2\pi M)^{N/2}\sigma^N} \exp\left\{-\frac{1}{2}\sum_{i=0}^{N-1} \frac{(z_{i+\nu} - M\eta_i)^2}{M\sigma^2}\right\}, \tag{6.36}$$

где подстрочные индексы у $z_{i+\nu}$ берутся по модулю N. Эта функция максимизируется с помощью отыскания максимума величины

$$v_\nu = \sum_{i=0}^{N-1} \eta_i z_{i+\nu}\,. \tag{6.37}$$

---

[1]) Когда N велико по сравнению с n, ошибка синхронизации может быть менее вредной, чем когда они более или менее равны. Это происходит потому, что в первом случае наиболее частая ошибка состояла бы в выборе некоторой метки, близкой к правильной метке. В некоторых случаях такие ошибки могут быть терпимы. Но так как время поиска зависит лишь логарифмически от P_e, это является слабым утешением. *(Прим. авт.)*.

Если $\eta_i = \eta_1$ для всех $i \neq 0$, имеем $v_\nu = (\eta_0 - \eta_1) z_\nu + \eta_1 \sum\limits_{i=0}^{N-1} z_i$, и v_ν максимизируется на том же самом ν, что и z_ν. Но для какого-либо другого множества средних значений η_i решение лишь на основе использования z_ν является подоптимальным. Решение, основанное на статистиках z_ν, а не на статистиках v_ν, будем называть *оптимальным задержанным решением.*

Статистики v_ν являются суммами гауссовских случайных величин и поэтому также распределены по Гауссу. В соответствии с этим вероятность P_e принять неправильную метку в случае, когда принимается оптимальное задержанное решение, может быть оценена обычным образом ($\nu = 0$ соответствует правильной метке) с помощью отношения

$$r^2 = \min_{\mu \neq 0} \frac{E^2(v_\mu - v_0)}{\operatorname{var}(v_\mu - v_0)} = \frac{M\left(\sum\limits_{i=0}^{N-1} (\eta_{i+\mu} - \eta_i)\,\eta_i\right)^2}{\sigma^2 \sum\limits_{i=0}^{N-1} (\eta_{i+\mu} - \eta_i)^2} \tag{6.38}$$

[ср. с (6.16)]. Когда сигнал имеет вид, задаваемый равенством (6.33), минимум отношений $E^2(v_\mu - v_0)/\operatorname{var}(v_\mu - v_0)$ достигается при $\mu = 1$. Таким образом, объединяя равенства (6.17), (6.18) и (6.38) и, для упрощения результата, считая N/n целым числом, находим, что требуемое время поиска равно $M_T T_0$ секунд, где

$$M_T = 2N^2 K_N \log_e (1/P_e)/nR. \tag{6.39}$$

Поиск с оптимальным задержанным решением определенно лучше ранее рассмотренных методов поочередного поиска, когда N велико по сравнению с n (т. е. когда требуемое разрешение во времени мало по сравнению с шириной импульса, используемого в синхроканале). Конечно, когда N равно n, оптимальный метод сводится к описанному ранее задержанному поиску.

Последовательный поиск. Для того чтобы применить последовательный алгоритм поиска к рассматриваемой ситуации, необходимо лишь сравнить текущую сумму

$$Z_m = \sum_{j=1}^{m} \zeta_{\nu j} \triangleq \sum_{j=1}^{m} \log_e \frac{p(z_{\nu j} \mid \nu)}{p(z_{\nu j} \mid \bar{\nu})}, \tag{6.40}$$

с двумя порогами $\log_e A$ и $\log_e B$. Гипотеза H_ν (о том, что ν-я метка является правильной) принимается, если это отношение превосходит $\log_e A$ и отвергается, если оно падает ниже $\log_e B$. Если ни одно из этих событий не имеет места, тест продолжается, новая статистика $\zeta_{\nu,\, m+1}$ добавляется к текущей сумме и Z_{m+1} сравнивается с теми же порогами.

Так как тест отношения правдоподобия является здесь равномерно наиболее мощным, то сложная альтернативная гипотеза будет заменена простой гипотезой $H_{\bar{\nu}}$ для некоторого $\bar{\nu} \neq \nu$. Вероятность ошибочного принятия некоторой частной метки является, конечно, функцией проверяемой метки. А именно, вероятность принятия μ-й метки

$$P_{\mu} = \frac{1 - B^{h(\mu)}}{A^{h(\mu)} - B^{h(\mu)}}, \tag{6.41}$$

где A и B пороги решения, а $h(\mu)$ — ненулевое решение уравнения $E(e^{h\varsigma_{\nu j}} \mid \mu) \triangleq g(h) = 1$.

В рассматриваемом здесь случае $p(z_{\nu j}|\nu) = (1/\sqrt{2\pi}\sigma) \times \times \exp\{-[(z_{\nu j} - \eta_0)^2/2\sigma^2]\}$; $p(z_{\nu j}|\bar{\nu}) = (1/\sqrt{2\pi}\sigma)\exp\{-[(z_{\nu j} - \eta_i)^2/2\sigma^2]\}$; $i = \nu - \nu$ по модулю N. Предположим на время, что $p(z_{\nu j}|\mu) = = (1/\sqrt{2\pi}\sigma')\exp\{-[(z_{\nu j} - \eta)^2/2(\sigma')^2]\}$. Тогда $h(\mu)$ является ненулевым решением уравнения

$$1 = g(h) = \frac{e^{f(h)}}{\sqrt{2\pi}\,\sigma'} \int_{-\infty}^{\infty} e^{-[(\xi - \eta')^2/2(\sigma')^2]}\, d\xi = e^{f(h)},$$

где $\eta' = \eta + h(\sigma'/\sigma)^2(\eta_0 - \eta_i)$ и $f(h) = [(\eta_0 - \eta_i)/2\sigma^2]h[2\eta + (\eta_0 - \eta_i) \times \times (\sigma'/\sigma)^2 h - (\eta_0 + \eta_i)]$. Так как последнее равенство справедливо для любого конечного значения h, необходимым условием того, что $g(h)$ равно единице, является равенство $f(h)$ нулю, и поэтому, если $h \neq 0$ и $\eta_i \neq \eta_0$,

$$h = h(\mu) = \frac{(\eta_0 + \eta_i) - 2\eta}{\left(\frac{\sigma'}{\sigma}\right)^2 (\eta_0 - \eta_i)}. \tag{6.42}$$

Если $\sigma' \leqslant \sigma$ и $\eta \leqslant \eta_i$, то $h(\mu) \geqslant 1$. Аналогично, если α и β являются параметрами, определяющими пороги A и B (см. § 2.4), $P_{\mu} \leqslant \beta$. Более того, если $\sigma' \leqslant \sigma$ и $\eta \geqslant \eta_0$, то $h(\mu) \leqslant -1$ и в этом случае $P_{\mu} \geqslant 1 - \alpha$.

Поэтому условия, приводящие к равенствам (2.44) и (2.48) удовлетворяются здесь, если $\eta_i = \max\limits_{l \neq 0} \eta_l = \eta_0 \rho$ и $\sigma' = \sigma$[1]. Так как в этом случае

$$\zeta_{\nu j} = \frac{\eta_0(1-\rho)}{\sigma^2} z_{\nu j} - \frac{\eta_0^2(1-\rho^2)}{2\sigma^2},$$

то

$$E(\zeta_{\nu j}|\mu) = R(1-\rho)[2\rho_i - (1+\rho)], \tag{6.43}$$

где $i = \nu - \mu$ по модулю N, $\rho = \max\limits_{i \neq 0} \rho_i$, а R и ρ_i определены ранее.

---

[1] Заметим, что если оценки величин η_0, ρ и σ являются осторожными, если действительное значение величины η_0, по крайней мере, не меньше ее предполагаемого значения, если $\rho_i < \rho$ для всех $i \neq 0$ и если истинная дисперсия не больше, чем σ, то тест, по меньшей мере, имеет такую надежность, которая ему приписывается. *(Прим. авт.)*.

Математическое ожидание времени, необходимого для завершения поиска, равно поэтому $\overline{M}_T T_0$, где

$$\overline{M}_T = \frac{C}{R(1-\rho)} \sum_{i=1}^{N-1} \frac{1}{(1+\rho-2\rho_i)} + \frac{\left(\log_e \frac{N-1}{P_e} - c\right)}{R(1-\rho)^2} \tag{6.44}$$

и где $C=c=1$ при $\alpha \to 0$, $\beta \to 0$ $(P_e \ll 1)$ и $C = \frac{1}{2} \log_e \frac{2}{P_e}$; $c=0$ при $\alpha = P_e/2$; $\beta = P_e/(N-1)$ $(P_e \ll 1)$ [ср. с равенствами (2.44) и (2.48)].

Последовательный поиск должен давать значительный выигрыш по сравнению с поиском с фиксированным объемом выборки, например, когда синхросигнал имеет вид (6.33), где N велико по сравнению с n. В этом случае одни метки намного легче устранить, чем другие. Поиск с фиксированным объемом выборки должен отводить одно и то же количество времени для проверки каждой метки, а при последовательном поиске можно тратить меньше времени на те метки, статистики которых значительно отличаются от статистик правильной метки. Равенство (6.44) в этом случае (в предположении, что N/n — целое число) имеет вид

$$\overline{M}_T \approx \frac{2C}{R}\left(\frac{N}{n}\right)^2 \left[1 + \log_e\left(\frac{2N}{n} - 1\right) + \frac{(N - 2N/n - 1)}{4(N/n - 1/2)} + \right.$$
$$\left. + \frac{1}{R}\left(\frac{N}{n}\right)^2 \left(\log_e \frac{N-1}{P_e} - c\right)\right. . \tag{6.45}$$

Таким образом, когда n мало, последовательный поиск с малым значением α, на самом деле, имеет худшие характеристики, чем метод оптимального задержанного решения. При $\alpha \to 1$ последовательный поиск имеет лучшие характеристики для всех $n \geqslant 2$, хотя при малых n это преимущество крайне мало. В другом крайнем случае, когда $n=N$, последовательный поиск приближенно в четыре раза быстрее, чем поиск с фиксированным объемом выборки при $\alpha = P_e/2$ и быстрее в $2\log_e(2/P_e)$ раз при $\alpha \to 1$.

6.5. Оценка меток

Хотя задача синхронизации в предыдущем параграфе трактовалась как задача проверки гипотез, ее можно (и целесообразно, когда ограничения на сложность устройства делают невозможной одновременную обработку) сформулировать в виде задачи оценки, рассматривая $\tau = \nu \Delta T$ как непрерывный параметр. В действительности в некоторых случаях, например, когда N очень велико или когда не требуется общая временна́я синхронизация, предположение о том, что число конкурирующих меток конечно, является до некоторой степени искусственным.

Если τ — непрерывный параметр, его оценка максимального правдоподобия удовлетворяет уравнению правдоподобия

$$\frac{\partial \log_e p[y(t) \mid \tau]}{\partial \tau} = \frac{2A}{N_0} \int_0^{MT_0} y(t) \frac{\partial}{\partial \tau} x(t+\tau)\, dt = 0. \tag{6.46}$$

Если это уравнение не может быть явно решено относительно τ, то ограничения на обработку обычно заставляют либо использовать устройство типа системы ФАПЧ для того, чтобы найти его решение, либо рассматривать только конечное множество меток τ. Оба эти подхода уже были исследованы в предыдущих параграфах этой главы.

Однако для некоторых сигналов $x(t)$ (6.46) может быть решено относительно τ. Например, предположим, что $x(t)$ синусоида $x(t)=\sqrt{2}\sin\omega_0 t$, где $\omega_0=2\pi/T_0$. Тогда

$$\frac{\partial \log_e p\,[y(t)\mid\tau]}{\partial\tau}=2R\,\omega_0\,[-X\sin\omega_0\tau+Y\cos\omega_0\tau], \tag{6.47}$$

где

$$\begin{Bmatrix}X\\ Y\end{Bmatrix}=\frac{1}{AT_0}\sum_{i=0}^{M-1}\int_{iT_0}^{(i+1)T_0}y(t)\sqrt{2}\begin{Bmatrix}\sin\omega_0 t\\ \cos\omega_0 t\end{Bmatrix}dt\overset{\Delta}{=}\sum_{i=0}^{M-1}\begin{Bmatrix}X_i\\ Y_i\end{Bmatrix}$$

и $R=A^2T_0/N_0$. Поэтому оценка максимального правдоподобия имеет вид

$$\hat{\tau}=\frac{T_0}{2\pi}\,\mathrm{arctg}\left(\frac{Y}{X}\right). \tag{6.48}$$

Среднее и дисперсия этой оценки могут быть легко определены из соответствующих результатов § 3.7. Для наших целей достаточно напомнить, что $\hat{\tau}$ как оценка максимального правдоподобия является асимптотически несмещенной и имеет дисперсию

$$E\,[(\hat{\tau}-\tau)^2\mid\tau]=\frac{1}{4R^2\,\omega_0^2\,ME\,[-X_i\sin\omega_0\tau+Y_i\cos\omega_0\tau]^2}=\frac{T_0^2}{(2\pi)^2\,2RM}. \tag{6.49}$$

Сделаем попытку найти другие синхросигналы, которые, подобно синусоидальному сигналу, позволяют уменьшить сложность устройств, но, как мы надеемся, приведут к лучшим характеристикам. Такое упрощение, очевидно, возможно, если функция $z(t+\tau)=\partial x(t+\tau)/\partial\tau$ является *разложимой* в том смысле, что она выражается в виде

$$z(t+\tau)=\sum_{i=1}^{n}f_i(t)\,g_i(\tau). \tag{6.50}$$

Если это можно сделать, то потребуется определить лишь n интегралов, и оценка величины τ получается в результате решения уравнения

$$\sum_{i=1}^{n}I_i g_i(\tau)=0, \tag{6.51}$$

где $I_i=\int\limits_0^{MT_0}y(t)f_i(t)\,dt$ [ср. с (6.46)]. Чтобы сложность устройства могла быть уменьшена на самом деле, n должно быть малым, а ур-ние (6.51) должно относительно просто решаться.

В любом случае, так как $z(t+\tau)$ — периодическая функция времени, ее можно разложить в ряд Фурье:

$$z(t+\tau)=\sum_{l=1}^{n/2} a_l \sin[\omega_l(t+\tau)+\theta_l]=$$

$$=\sum_{l=1}^{n/2}[a_l \sin\omega_l t\cos(\omega_l\tau+\theta_l)+a_l\cos\omega_l t\sin(\omega_l\tau+\theta_l)], \qquad (6.52)$$

где $\omega_\nu=2\pi k_\nu/T_0$ и T_0 — период $z(t)$, а k_ν — целое число. Функции $f_\nu(t)$ и $g_\nu(\tau)$ из равенства (6.50) можно поэтому определить следующим образом:

$$f_\nu(t)=\begin{cases}\sin\omega_{(\nu+1)/2}\,t, & \nu \text{ — нечетное;}\\ \cos\omega_{\nu/2}\,t, & \nu \text{ — четное}\end{cases} \qquad (6.53)$$

и

$$g_\nu(\tau)=\begin{cases}a_{(\nu+1)/2}\cos(\omega_{(\nu+1)/2}\tau+\theta_{(\nu+1)/2}), & \nu\text{—нечетное;}\\ a_{\nu/2}\sin(\omega_{\nu/2}\tau+\theta_{\nu/2}), & \nu \text{ — четное.}\end{cases}$$

Так как I_i из (6.51) статистически независимы, когда функции $f_\nu(t)$ определены согласно (6.53), то в этом методе требуется вычисление, по меньшей мере n корреляций. Предположим противоположное, что интеграл в ф-ле (6.46) мог быть выражен в виде $\sum_{j=1}^{m} J_j g'_j(\tau)$ для некоторого множества функций $g'_j(\tau)$ при $m<n$. Тогда

$$\sum_{i=1}^{n} I_i g_i(\tau)=\sum_{j=1}^{m} J_j g'_j(\tau),$$

и так как функции $g_i(\tau)$ ортогональны на интервале $(0,\ T_0)$ то

$$I_\nu=\sum_{i=1}^{m}\alpha_{\nu j}J_j, \quad \nu=1,2,\ldots,n,$$

где $$\alpha_{\nu j}\triangleq\int_0^{T_0} g'_j(\tau)\,g_i(\tau)d\tau \Big/ \int_0^{T_0} g_i^2(\tau)\,d\tau.$$

Но в этом случае переменные J_j могли бы быть выражены как линейные комбинации первых m переменных I_ν (если эти переменные являются линейно независимыми). Это, в свою очередь, означало бы, что существует линейное соотношение между некоторыми из переменных I_ν и поэтому приводило бы к противоречию.

Мы уже обсуждали характеристику синхронизатора, когда функция $z(t)$ определялась равенством (6.52), а $n=2$. В предыдущем абзаце говорилось о том, что эта характеристика не может быть улучшена без использования бо́льшего числа корреляторов. Если n больше двух, результирующее уравнение максимального правдоподобия (6.51), на первый взгляд, является достаточно сложным, что ограничивает его применимость. Однако это ограничение можно преодолеть с помощью раздельного решения каждого из уравнений $l_\nu\, g_\nu(\tau)+l_{\nu+1}\, g_{\nu+1}(\tau)=0$, ν — нечетное и использования решения уравнения, соответствующего максимальной частоте ω_ν, для того чтобы найти оценку $\hat{\tau}$ величины τ. Решение остальных уравнений можно затем использовать для устранения остающихся неопределенностей. Получающаяся в результате оценка хотя и является подоптимальной, вообще говоря, несущественно отличается от оптимальной оценки. В § 6.9 подробно обсуждается незначительная модификация этой схемы, которая приводит к особенно простой реализации.

В действительности довольно эффективные формулы оценок могут быть иногда построены при использовании статистик, отличных от тех, которые получаются из ур-ния (6.46). Например, предположим, что синхросигнал представляет собой периодическую последовательность прямоугольных импульсов длительности $T_0/2$. Автокорреляционная функция такого сигнала изображена на рис. 6.2. Заметим что каждое значение $\rho(\tau)$ из области (0, 1) соответствует только двум возможным значениям τ из интервала $(0,\ T_0)$. (Если $\rho(\tau)=1$, то значение τ однозначно определяется по модулю T_0.) В соответствии с этим хорошую оценку функции $\rho(\tau)$ можно было бы использовать для оценки τ и далее для оценки правильной метки (точки $\tau=0$). Так как

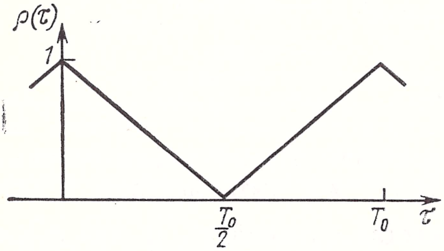


Рис. 6.2. Периодическая автокорреляционная функция последовательности прямоугольных импульсов ширины $T_0/2$

$$\rho(\tau)=1-\frac{2\,|\tau|}{T_0};\quad |\tau|<\frac{T_0}{2}, \tag{6.54}$$

то, разрешая уравнение относительно $|\tau|$, получаем

$$|\tau|=\frac{T_0}{2}\,[1-\rho(\tau)]. \tag{6.55}$$

Оценим теперь $\rho(\tau)$ с помощью

$$\hat{\rho}(\tau)=\frac{1}{MAT_0}\int\limits_0^{MT_0} y(t)\,x(t)\,dt, \tag{6.56}$$

где функция $x(t)$ определена равенством (6.33) (с $n=2$) и $y(t)=$

$=Ax(t-\tau)+n(t)$, и затем в качестве оценки $|\tau|$ использовать величину

$$\widehat{|\tau|}=\frac{T_0}{2}[1-\hat{\rho}(\tau)]. \tag{6.57}$$

Формула оценки максимального правдоподобия, если она существует, величины $|\tau|$ при условии, что задана наблюдаемая $\hat{\rho}(\tau)$, как раз и определяется соотношением (6.57). При этом во всех точках, кроме точек разрыва производной $d\rho(\hat{\tau})/d\hat{\tau}$, имеем

$$0=\frac{\partial \log p[\hat{\rho}(\tau)\mid\hat{\tau}]}{\partial\hat{\tau}}=\pm k[\hat{\rho}(\tau)-\rho(\hat{\tau})], \tag{6.58}$$

где k — постоянная, не зависящая от $\hat{\tau}$. Это уравнение имеет единственное решение $\hat{\rho}(\tau)=\rho(\hat{\tau})$. Поэтому если $|\hat{\rho}(\tau)|\leqslant 1$, то оценкой максимального правдоподобия величины $|\tau|$ будет $\widehat{|\tau|}$, где

$$\rho(\hat{\tau})=1-\frac{2\widehat{|\tau|}}{T_0}=\hat{\rho}(\tau). \tag{6.59}$$

Так как $\hat{\rho}(\tau)$ имеет гауссовское распределение, то $\widehat{|\tau|}$ имеет то же распределение со средним и дисперсией, задаваемыми равенствами:

$$\eta_{\hat{\tau}}=E(\widehat{|\tau|})=(T_0/2)[1-E(\hat{\rho}(\tau))]=(T_0/2)[1-\rho(\tau)]=|\tau|; \tag{6.60}$$

$$\sigma^2_{\hat{\tau}}=\operatorname{var}(\widehat{|\tau|})=(T_0/2)^2\operatorname{var}[\hat{\rho}(\tau)]=\frac{T_0^2}{8MR} \tag{6.61}$$

соответственно.

Этот метод оценки весьма близок как в смысле сложности требуемого устройства, так и в смысле получаемых результатов, к оценке максимального правдоподобия меток синусоидального сигнала [ср. равенства (6.49) и (6.61)]. Это может показаться удивительным, так как последняя является оценкой максимального правдоподобия, основанной на наблюдаемых $y(t)$, в то время как первая является оценкой максимума правдоподобия, использующей лишь статистику $\hat{\rho}(\tau)$. На самом деле, если наблюдаемые $y(t)$ используются оптимально вместе с сигналом, имеющим автокорреляционную функцию (6.54), то получаются намного лучшие результаты. Время, необходимое для обнаружения правильной метки среди N конкурирующих меток, можно уменьшить примерно в N раз по сравнению со временем, необходимым для оценивания (ср. с § 6.4).

Для того чтобы сопоставить эти результаты более детально с результатами метода различения гипотез, полученными в предыдущих параграфах, будем считать, что ошибка синхронизации происходит, если оценка $\widehat{|\tau|}$ отличается от $|\tau|$ более чем на $\Delta T/2 = T_0/2N$ секунд. Тогда

$$P_e = 1 - \operatorname{erf}(M^{1/2}R^{1/2}/N),$$

и время поиска будет порядка $M_T T_0$, где

$$M_T = \frac{N^2}{R} \log_e \frac{1}{P_e}. \tag{6.62}$$

Поиск, однако, на этом не заканчивают, так как до сих пор мы оценили лишь $|\tau|$, а не τ. Необходимо дополнительное наблюдение, чтобы определить, какая оценка, $\hat{\tau} = \widehat{|\tau|}$ или $\hat{\tau} = -\widehat{|\tau|}$, лучше. Это можно решить, например, используя тест с фиксированным объемом выборки относительно меток $\tau = \widehat{|\tau|}$ и $\tau = -\widehat{|\tau|}$ и принимая ту, которая дает наибольшую корреляцию. Число наблюдаемых необходимых для решения, когда две метки исследуются поочередно, может доходить до $M' = (N^2/R)\log_e(1/P_e)$ [ср. с (6.33)]. Это число, в силу иронии, равно тому, которое необходимо для первоначальной оценки. Вместе с тем, если обе конкурирующие метки можно обрабатывать одновременно, используя лишь два коррелятора, необходимое число наблюдаемых согласно ф-ле (6.19) будет самое большее порядка $M'' = M'/N$, что при больших N дает пренебрежимо малое увеличение общего времени оценивания.

Следует признать, что метод оценки меток более существенно зависит от точного знания амплитуды сигнала, чем другие рассмотренные до сих пор методы. Если амплитуда сигнала не известна, она должна быть оценена либо до поиска, либо в процессе поиска. В любом случае неизбежные ошибки этой оценки будут увеличивать вероятность ошибки окончательного решения. Этот недостаток может быть в какой-то мере устранен, если имеются опорные отсчеты времени. Если амплитуда принятого сигнала времени находится в некотором известном соотношении с амплитудой синхросигнала, то оценка амплитуды может быть получена как побочный результат, связанный с наличием опорных отсчетов времени. Таким образом, это предварительное условие для успешного применения процедуры оценки меток может оказаться менее жестким, чем можно было бы ожидать.

6.6. Фазовонекогерентная синхронизация

Может случиться так, что синхронизация должна быть достигнута без априорного знания фазы несущей канала синхронизации. Это происходит либо тогда, когда ограничения, накладываемые на систему, делают невозможным когерентный прием, либо тогда, когда по какой-то причине более выгодно сначала установить синхронизацию, а затем фазовую когерентность. Следует заметить, что наличие отсчетов времени еще не обеспечивает фазовую когерентность. Если, например, частота несущей намного больше частоты отсчета времени, то отсчеты времени, по существу, не дают никакой информации относительно фазы несущей. В некоторых случаях можно даже установить синхронизацию без всякого общего отсчета времени, если при этом временна́я неопределенность на передатчике достаточно мала, чтобы можно было пренебречь ею в процессе синхронизации. Некоторые методы синхронизации, развитые в предыдущих параграфах, вновь рассматриваются здесь применительно к фазовонекогерентным каналам.

Некогерентный по фазе приемник максимального правдоподобия рассматривался в гл. 3 и 4. Если можно предположить, что фаза практически остается постоянной, по крайней мере, в течение любого заданного интервала T_0 секунд, то некогерентный по фазе синхронизатор максимального правдоподобия должен вычислять выражения

$$\int_0^{2\pi} \ldots \int_0^{2\pi} p(\Phi_0, \Phi_1 \ldots, \Phi_{M-1}) \times$$

$$\times \left[\prod_{l=0}^{M-1} \exp \frac{2A}{N_0} \int_{lT_0}^{(l+1)T_0} y(t)\, s_\nu(t, \Phi_l)\, dt \right] d\Phi_0\, d\Phi_1 \ldots d\Phi_{M-1}, \qquad (6.63)$$

где $\{s_\nu(t, \Phi) = \sqrt{2}\, \xi(t - \nu\Delta T) \sin[\omega_c(t - \nu\Delta T) + \theta(t - \nu\Delta T) + \Phi]\}$ означает множество возможных принимаемых сигналов синхронизации, а $y(t) = As_r(t, \Phi) + n(t)$ — принимаемый сигнал, сложенный с шумом. Это выражение пропорционально апостериорной вероятности ν-й метки при заданном сигнале $y(t)$, $0 < t < MT_0$.

Выражение (6.63) выглядит довольно громоздким, даже если точно известна M-мерная плотность распределения $p(\Phi_0, \Phi_1, \ldots, \Phi_{M-1})$. Эта плотность распределения отражает, среди прочего, скорость, с которой фаза принимаемой несущей уходит по отношению к местной опорной фазе. В большинстве случаев ее можно определить лишь приближенно. Чтобы обойти эту трудность, ограничимся здесь рассмотрением двух крайних случаев:

$$p(\Phi_0, \Phi_1, \ldots, \Phi_{M-1}) = p(\Phi_0)\, \delta(\Phi_0 - \Phi_1)\, \delta(\Phi_0 - \Phi_2) \ldots \delta(\Phi_0 - \Phi_{M-1})$$

и $p(\Phi_0, \Phi_1, \ldots, \Phi_{M-1}) = p(\Phi_0)\, p(\Phi_1) \ldots p(\Phi_{M-1})$,

где $p(\Phi_i) = (1/2\pi)$; $0 \leqslant \Phi_i < 2\pi$. В первом случае фаза постоянна в течение периода синхронизации; во втором предполагается, что она принимает независимые значения на различных интервалах длиной T_0 секунд. Фазовонекогерентная синхронизация фактически означает, что должны одновременно оцениваться метка принимаемого сигнала и фаза его несущей, хотя последняя явно не оценивается. Чем дольше фаза остается постоянной, тем лучше она может быть оценена и, следовательно, тем лучше может быть оценена метка. Два рассматриваемых случая соответствуют поэтому двум крайним значениям потенциальной характеристики синхронизатора[1]). Выражение (6.63) в этих условиях, соответственно, имеет следующий вид (ср. с § 4.3; как и там, предполагается, что $\omega_c \gg 2\pi/T_0$):

— в первом случае

$$\frac{1}{2\pi}\int\limits_0^{2\pi} \exp\frac{2A}{N_0}\int\limits_0^{MT_0} y(t)\, s_\nu(t,\Phi)\, dt\, d\Phi = I_0(2MRw_\nu); \qquad (6.64)$$

где $w_\nu = (a_\nu^2 + b_\nu^2)^{1/2}$; $R = \mathscr{E}/N_0$; $\mathscr{E} = A^2 \int\limits_0^{T_0} s_\nu^2(t,\Phi)\, dt \triangleq A^2 \mathscr{E}_0$;

$$a_\nu = \frac{1}{M}\sum_{l=0}^{M-1} a_{\nu l}; \quad a_{\nu l} = \frac{A}{\mathscr{E}}\int\limits_{lT_0}^{(l+1)T_0} y(t)\, s_\nu(t,\, 0)\, dt;$$

$$b_\nu = \frac{1}{M}\sum_{l=0}^{M-1} b_{\nu l}; \quad b_{\nu l} = \frac{A}{\mathscr{E}}\int\limits_{lT_0}^{(l+1)T_0} y(t)\, s_\nu\left(t,\, \frac{\pi}{2}\right) dt;$$

во втором случае

$$\prod_{l=0}^{M-1} \frac{1}{2\pi}\int\limits_0^{2\pi} \exp\left(\frac{2A}{N_0}\int\limits_{lT_0}^{(l+1)T_0} y(t)\, s_\nu(t,\, \Phi_l)\, dt\, d\Phi_l = \sum_{l=0}^{M-1} I_0(2Rz_{\nu l}) \triangleq z_\nu, \right. \qquad (6.65)$$

где $z_{\nu l} = (a_{\nu l}^2 + b_{\nu l}^2)^{1/2}$.

В первом случае w_ν сама может быть использована как решающая переменная, так как $I_0(2MRw_\nu)$ — монотонная функция w_ν. Рассмотрения § 4.3 показывают, что

$$p(w_\nu \mid \mu) = \begin{cases} 2MR\, w_\nu \exp[-MR(w_\nu^2 + \rho_i^2)]\, I_0(2MR\, \rho_i w_\nu); & w_\nu > 0. \\ 0 & w_\nu < 0, \end{cases} \qquad (6.66)$$

где $i = \mu - \nu$; $\rho_i^2 = \tilde{\rho}_i^2 + \hat{\rho}_i^2$; $\tilde{\rho}_i = \frac{1}{\mathscr{E}_0}\int\limits_0^{T_0} s_0(t,\, 0)\, s_i(t,\, 0)\, dt$ и $\hat{\rho}_i = \frac{1}{\mathscr{E}_0} \times$ $\times \int\limits_0^{T_0} s_0(t,0)\, s_i(t,\pi/2)\, dt$. Результаты этого параграфа могут быть здесь применены непосредственно. Например, если $\tilde{\rho}_i$ и $\hat{\rho}_i$ равны нулю для всех $i \neq 0$, вероятность правильного решения задается равенством (4.45) (где R следует заменить на MR). Остальные результаты § 4.3, включая границы для произвольных ρ_i, также могут быть использованы здесь.

---

[1] Фаза, конечно, могла бы меняться даже внутри интервала в T_0 секунд, что приводило бы к еще большему ухудшению характеристики. Однако на практике эта ситуация маловероятна, по крайней мере, когда T_0 — период символа. Если T_0 соответствует синхронизационному интервалу более высокого порядка, то полезно использовать известную последовательность символов в качестве сигнала синхронизации и использовать метод, рассматриваемый здесь, для символьной синхронизации, а также применить методы синхронизации слов, изложенные в последующих главах, для того чтобы снять оставшиеся неоднозначности. Если синхросигнал представляет собой импульс длительности T_0/n, то, конечно, единственное, что необходимо для удовлетворения второго условия — это относительное постоянство фазы на каждом интервале в T_0/n секунд. *(Прим. авт.)*.

Поиск с фиксированным объемом выборки основан на использовании отношения плотностей вероятностей вида

$$\frac{p(w_\nu \mid \nu)}{p(w_\nu \mid \mu)} = \frac{e^{-MR} I_0(2MRw_\nu)}{e^{-MR\rho_i^2} I_0(2MR\rho_i w_\nu)}. \tag{6.67}$$

Можно показать, что отношение $I_0(ax)/I_0(bx)$ — монотонно возрастающая функция x при $a > b$. Так как $\rho^2_i < 1$ для всех $i \neq 0$, то тест отношения плотностей вероятностей является односторонним тестом w_ν; ν-я метка принимается тогда и только тогда, когда w_ν превышает некоторую фиксированную величину. Следовательно, тест является равномерно наиболее мощным, и выбор альтернативной гипотезы несуществен. Вероятность ошибки первого рода согласно § 4.3 ($\nu = 0$ — правильная метка) имеет вид

$$\alpha = 1 - \int_\theta^\infty p(w_0)\,dw_0 = 1 - Q\left[(2MR)^{1/2};\ (2MR)^{1/2}\theta\right], \tag{6.68}$$

где $Q(x, y)$ определена в ф-ле (4.47), а θ такова, что когда $w_\nu > \theta$, отношение (6.67) превышает требуемый порог. Аналогично для вероятности ошибки второго рода имеем

$$\beta_\nu = \int_\theta^\infty p(w_\nu)\,dw_\nu = Q\left[(2MR)^{1/2}\rho_\nu, (2MR)^{1/2}\theta\right]. \tag{6.69}$$

Если $\tilde{\rho}_\mu$ и $\hat{\rho}_\nu$ равны нулю для всех $\nu \neq 0$ — случай ортогональных сигналов, то

$$\beta_\nu = Q\left[0,\ (2MR)^{1/2}\theta\right] = e^{-MR\theta^2}. \tag{6.70}$$

Таким образом, можно, например, приравнять P_e к $\alpha + [(N-1)/2]\beta$ и выбрать θ так, чтобы минимизировать вероятность ошибки в § 6.5.

К сожалению, условия, необходимые для справедливости выводов, касающихся длительности последовательного теста отношения плотностей вероятностей (§ 2.3), здесь не удовлетворяются. А именно, отношение $p(w_\nu \mid \nu)/p(w_\nu \mid \mu)$ не может быть выражено в виде произведения отношений вида $p(w_{\nu l} \mid \nu)/p(w_{\nu l} \mid \mu)$. Такое разложение означало бы пренебрежение зависимостью фазы несущей на последовательных интервалах. Если бы такая зависимость не существовала, то решающие переменные были бы такими, как в рассмотренном выше втором случае. При анализе последовательного поиска в этом последнем случае мы, конечно, одновременно строим границу снизу для характеристики последовательного поиска, основанного на использовании решающих переменных w_ν. То же утверждение справедливо и для других процедур поиска. Более того, анализ когерентной синхронизации, содержащийся в предыдущих параграфах, дает верхние границы для характеристики, которая получается при использовании статистик w_ν.

Теперь непосредственно перейдем к анализу характеристики синхронизатора во втором случае. Поиск должен быть основан на использовании статистик z_ν, определяемых равенством (6.65), или, что более удобно, статистик

$$\log z_\nu = \sum_{l=0}^{M-1} \log I_0(2R z_{\nu l}) . \tag{6.71}$$

Так как $\log z_\nu$ — сумма большого (по предположению) числа независимых случайных величин, то удовлетворяются условия, необходимые для применимости центральной предельной теоремы[1]), и $\log z_\nu$ приближенно имеет гауссовское распределение. Этот факт можно использовать для упрощения анализа, когда статистики z_ν являются решающими переменными. Однако на приемном конце, вообще говоря, неудобно вычислять функции Бесселя. Следующее замечание приводит к простой и математически удобной аппроксимации $\log z_\nu$. Наиболее трудная ситуация, очевидно, будет тогда, когда отношение сигнал/шум $R = \mathcal{E}/N_0$ мало. Если это отношение велико, то почти любая система синхронизации будет работать удовлетворительно. Но если R мало по сравнению с единицей, то имеем

$$\log_e [I_0(2Rz_{\nu l})] \approx \log_e (1 + R^2 z_{\nu l}^2) \approx R^2 z_{\nu l}^2, \tag{6.72}$$

и решение можно построить на основе использования суммы квадратов величин $z_{\nu l}$, а не суммы функций Бесселя от этих величин, что приводит к значительному упрощению[2]).

Определим

$$\zeta_\nu = \sum_{l=0}^{M-1} z_{\nu l}^2 . \tag{6.73}$$

Здесь опять ζ_ν — сумма большого числа независимых случайных величин, и согласно центральной предельной теореме она имеет приближенно гауссовское распределение. Напомним, что большинство границ для времени решения, полученных в предыдущих параграфах этой главы, зависит единственно от отношений вида

---

[1]) Существование вторых моментов одинаково распределенных случайных величин $\log I_0(2Rz_{\nu l})$ является достаточным условием для справедливости этого утверждения. *(Прим. авт.)*.

[2]) В другом крайнем случае, когда R велико по сравнению с единицей $\zeta_{\nu l} = \log_e I_0(2Rz_{\nu l}) \approx 2Rz_{\nu l}$ и можно было бы использовать сумму самих $z_{\nu l}$. Но, как увидим, характеристика системы, использующей сумму квадратов величин $z_{\nu l}$, лишь немного хуже характеристики когерентной системы в случае, когда R велико. Таким образом, возможное преимущество использования приближения к идеальному синхронизатору с большим отношением сигнал/шум, по-видимому, невелико. *(Прим. авт.)*.

$$r^2 = \min_{\nu \neq 0} \frac{E^2 (x_0 - x_\nu)}{\operatorname{var} (x_0 - x_\nu)},$$

где x_ν — гауссовские случайные величины, соответствующие ν-й метке (нулевая метка является правильной). В рассматриваемом случае[1])

$$E(\zeta_\nu) = M\left(\rho_\nu^2 + \frac{1}{R}\right); \tag{6.74}$$

$$\operatorname{var}(\zeta_\nu) = M\left[\frac{1}{R^2} + \frac{2}{R}\rho_\nu^2\right],$$

и если μ- и ν-я метки проверяются одновременно, то

$$\operatorname{var}(\zeta_\nu - \zeta_\mu) = 2M\left\{\frac{1}{R^2}(1 - \rho_i^2) + \right.$$

$$\left. + \frac{1}{R}\left[\rho_\nu^2 + \rho_\mu^2 - 2\tilde{\rho}_i\left(\hat{\rho}_\nu \hat{\rho}_\mu + \tilde{\rho}_\nu \tilde{\rho}_\mu\right) - 2\hat{\rho}_i\left(\hat{\rho}_\nu \tilde{\rho}_\mu - \tilde{\rho}_\nu \hat{\rho}_\mu\right)\right]\right\}, \tag{6.75}$$

где ${\rho^2}_j = \tilde{\rho}^2{}_j + \hat{\rho}^2{}_j$ и $i = \nu - \mu$ по модулю N. Используя, например, границы (6.17), (6.18), находим, что время, необходимое для решения при параллельных наблюдениях, имеет порядок $M_T T_0$ секунд, где

$$M_T = \frac{4k_N \quad \log_e (1 / P_e)}{(1 - \rho^2)\, R^2/(R + 1)} \tag{6.76}$$

и $\rho^2 = \max\limits_{\nu \neq 0} \rho_\nu^2$. Аналогично время, требующееся для поиска с фиксированным объемом выборки, равно приближенно $\overline{M}_T T_0$, с, где

$$\overline{M}_T = \frac{4Nk_N'' \log_e (1/P_e)}{(1 - \rho^2)^2 \{R^2/[R(1 + \rho^2) + 1]\}} \tag{6.77}$$

[см. (6.30)].

---

[1]) Для дальнейшего заметим также, что если известно, что Φ принимает одно из двух значений $\Phi = 0$ или $\Phi = \pi$, то решение должно основываться на статистике $\zeta_\nu' = \sum\limits_{l=0}^{n} a_{\nu l}^2$, а не на статистике ζ_ν, определяемой равенством (6.73). Кроме того,

$$E(\zeta_\nu') = M(\rho_\nu^2 + 1/2R)$$

и

$$\operatorname{var}(\zeta_\nu' - \zeta_\mu') = M\left\{\frac{1}{R^2}(1 - \rho_i^2) + \frac{2}{R}(\rho_\nu^2 + \rho_\mu^2 - 2\rho_i \rho_\mu \rho_\nu)\right\}.$$

(Прим. авт.).

Другие результаты предыдущего параграфа также могут быть обобщены на случай фазовонекогерентной синхронизации, Так, например, алгоритм последовательного поиска легче всего применить к настоящей задаче, если предположить, что статистики $z_{\nu l}^2$ имеют гауссовское распределение со средним $E(z_{\nu l}^2\,|\,\nu)=\eta_0$ и дисперсией $\sigma^2=\max\limits_{\mu}\operatorname{var}(z_{\nu l}^2\,|\,\mu)$, и выбирать в качестве альтернативной гипотетической метки метку $\bar{\nu}$, имеющую среднее $\eta_1=E(z_{\nu l}^2\,|\,\bar{\nu})=\max\limits_{\mu} E(z_{\nu l}^2\,|\,\mu)$ и дисперсию σ^2. При этом поиск будет основан на решающих переменных

$$\zeta_{\nu l}=\frac{\eta_0-\eta_1}{\sigma^2}\left\{z_{\nu l}^2-\frac{\eta_0+\eta_1}{2}\right\}.$$

Математическое ожидание времени поиска можно оценить, используя ф-лы (2.44) и (2.48). Вероятность ошибки, соответствующая этим выражениям, не представляет, конечно, действительной вероятности ошибки, так как наблюдаемые $z_{\nu l}^2$ не распределены по Гауссу. Однако результаты § 2.6 относительно влияния на уровень значимости и мощность теста того обстоятельства, что распределение наблюдаемых не соответствует ни нулевой, ни альтернативной гипотезам, могут быть использованы для отыскания действительной вероятности ошибки. [Распределение наблюдаемых $z_{\nu l}$ задается равенством (4.36)].

Хотя решающие переменные ζ_ν являются оптимальными только при очень малых отношениях сигнал/шум R, приятно заметить, что если R велико, получающееся в результате выражение для M_T [равенства (6.76) и (6.77)], когда $\rho=0$, лишь вдвое больше соответствующего выражения в случае когерентной синхронизации. Более того, если R велико, требуемое время поиска в обоих случаях становится одним и тем же при $\rho\to 1$. Так как характеристика синхронизатора, использующего величины w_ν [равенство (6.64)], ограничена характеристиками: сверху — когерентного синхронизатора и снизу — синхронизатора, использующего величины ζ_ν, то он должен приводить лишь к чуть лучшей характеристике, чем для синхронизатора с ζ_ν в только что рассмотренных условиях, даже когда фаза может предполагаться постоянной на полном интервале поиска MT_0 секунд. Наконец, можно заключить, что ухудшение характеристики за счет использования ζ_ν вместо $\log z_\nu$ мало́ независимо от отношения сигнал/шум R. Когда R велико, предыдущие замечания имеют силу; когда R мало, ζ_ν и $\log z_\nu$, по существу, равны, и любое улучшение при использовании последней величины будет пренебрежимо малым.

Зависимость времени поиска от числа меток N одна и та же как при когерентной, так и при некогерентной сихронизации. Зависимости времени поиска от отношения сигнал/шум R в этих двух случаях также, по существу, являются одинаковыми, если R велико по сравнению с единицей. Однако, когда R мало, характеристика фазовонекогерентного синхронизатора зависит как $1/R^2$ от этого параметра, а характеристика когерентного синхронизатора — как $1/R$.

До этого как закончить параграф, заметим также, что системы ФАПЧ могут быть иногда использованы с успехом даже тогда, когда синхронизацию нужно установить некогерентно. Например, прямоугольный импульс, рассмотренный в § 6.3, может быть отслежен системой ФАПЧ даже при отсутствии опорной несущей. Однако анализ характеристик такой цепи отложим на некоторое время, так как то же самое устройство будет вновь рассмотрено в большей общности в § 8.6.

6.7. Выбор синхросигнала. Псевдошумовые последовательности

Все рассмотренные в предыдущих параграфах схемы решения относительно меток приводили к таким выражениям для времени поиска или, по крайней мере, для границ этого времени поиска, которые были монотонно возрастающими функциями максимального коэффициента корреляции ρ (или в случае фазовонекогерентной синхронизации — значения ρ^2). В соответствии с этим, если мы свободны в выборе сигнала синхроканала, нужно, по-видимому, пытаться минимизировать этот параметр. Задача состоит в отыскании периодического сигнала $x(t)$ с периодом T_0, такого, что в множестве N сигналов $x_\nu(t)=x[t-(\nu T_0/N)]$, $\nu=0, 1, \ldots, N-1$ максимальный из коэффициентов корреляции

$$\rho_{\mu\nu}=\frac{1}{\mathscr{E}}\int\limits_0^{T_0} x_\mu(t)\,x_\nu(t)\,dt \qquad (6.78)$$

является по возможности наименьшим. Как было показано в § 4.2, неравенство

$$\max_{\substack{\mu,\ \nu\\ \mu\neq\nu}} \rho_{\mu\nu} \geqslant -\frac{1}{N-1} \qquad (6.79)$$

справедливо для любого множества N сигналов. Эта нижняя граница, очевидно, может быть использована здесь. Вскоре будет указан класс сигналов, на котором достигается эта граница. Но сначала заметим, что, когда N велико, ортогональное множество (с $\rho_{\mu\nu}=0$) почти оптимально (и вероятно оптимально в некогерентном случае). Сразу же можно предложить один класс ортогональных сигналов — сигналы ВИМ, рассмотренные в § 4.4: если $x(t)=\sqrt{2N}\sin\omega_c t$, $0\leqslant t\leqslant T_0/N$, то $\rho_{\mu\nu}=0$ для всех $\mu\neq\nu$, как и требуется.

Таким образом, почти оптимальный синхросигнал в случае, когда используется любая из процедур поиска, приведенных в предыдущих параграфах, представляет собой просто импульс с длительностью T_0/N, передаваемый каждые T_0 секунд. Основной недостаток такого сигнала состоит в том, что его амплитуда пропорциональна $\sqrt{N}$, и поэтому пиковая передаваемая мощность будет пропорциональна N, если требуется, чтобы общая передаваемая мощность оставалась постоянной. Это условие жестко ограничивает значение N в реальных системах и тем самым ограничивает возможность уменьшения первоначальной неоднозначности во времени.

К счастью, можно не только генерировать сигнал, имеющий, по существу, оптимальные коэффициенты корреляции $\rho_{\nu\mu}$ в отсутствие жесткого ограничения на пиковую мощность импульса сигнала, но и делать это при дополнительном условии, что его огибающая постоянна независимо от времени.

Рассмотрим следующую функцию[1]:

$$x(t)=\begin{cases}1, & 0<t<T_0/3;\\ 1, & T_0/3<t<2T_0/3;\\ -1, & 2T_0/3<t<T_0\end{cases} \tag{6.80}$$

Эта функция, график которой изображен на рис. 6.3*а*, может быть представлена последовательностью $\{1,\ 1,\ -1\}$. График автокорреляционной функции $\rho(\eta)$ приведен на рис. 6.3*б*. Отметим, что $\rho(\eta)$ изменяется линейно в интервалах между значениями, которые она принимает в точках $\eta=0$, $T_0/3$, $2T_0/3, \ldots$; чтобы полностью задать функцию, необходимо ее определить лишь в этих точках. Ясно, что этот случай всегда имеет место, когда $x(t)$ представляет собой последовательность импульсов постоянной амплитуды и одинаковой длительности ΔT секунд, т. е. всегда, когда $x(t)$ может быть представлена последовательностью $+1$ и -1. Функция, определенная равенством (6.80), в действительности чуть предпочтительней (для фазовокогерентного случая), чем прямоугольный

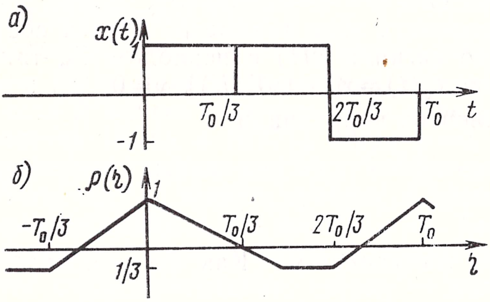


Рис. 6.3. Пример последовательности и ее автокорреляционной функции: *а)* функция $x(t)$ [см. (6.80)]; *б)* периодическая автокорреляционная функция

импульс с длительностью $\Delta T = T_0/3$. Но ее самое важное преимущество состоит в постоянстве уровня мощности.

---

[1] Действительный передаваемый сигнал обычно будет иметь вид $x(t)\sqrt{2}A\sin\omega_0 t$. Здесь предполагается, что демодуляция несущей уже выполнена. (*Прим. авт.*).

Желание получить меньшую эффективную длительность импульса приводит к необходимости строить более длинные последовательности $+1$ и -1, обладающие автокорреляционными функциями, которые достигают нижней границы (6.79). Заметим, что эффективная длительность импульса ΔT сигнала такого вида не может быть меньше, чем T_0/N, где N — число символов (в одном периоде) в двухуровневой последовательности, представляющей $x(t)$. Цель поэтому состоит в том, чтобы найти двухуровневую последовательность периода N, имеющую равномерно малую корреляционную функцию $\rho(\eta)$ для всех η из интервала $iT_0 + T_0/N < \eta < (i+1)T_0 - T_0/N$. Ниже будет показано, что это можно сделать для любого N вида $N = 2^k - 1$, где k — целое число.

Чтобы продемонстрировать процедуру формирования такой последовательности, укажем одно специальное свойство последовательности $\{1, 1, -1\}$, которое является ключевым для этого обобщения. Заменяя символ -1 в этой последовательности нулем, найдем, что сумма по модулю два первых двух символов равна третьему; сумма по модулю два второго и третьего символов равна первому и сумма по модулю два третьего и первого символов равна второму. Эта последовательность может быть порождена *линейным регистром сдвига с обратной связью,* его функциональная схема изображена на рис. 6.4*а*. Прямоугольники изображают элементы памяти, которые хранят *единицу* или *нуль* в течение одной единицы времени (в этом примере — $T_0/3$ секунд) и затем сдвигают их в направлении выходной стрелки. Цепь содержит элемент $\oplus$ — спецзнак, обозначает сумматор по модулю два; он мгновенно производит суммирование по модулю два его входов и подает сумму в направлении его выходной стрелки. Легко проверить, что этот регистр сдвига генерирует периодическую последовательность ...110110...

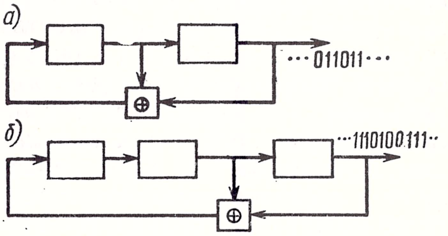


Рис. 6.4. Функциональные схемы генераторов последовательностей регистра сдвига

Таким образом, двухразрядный (т. е. с двумя элементами памяти) регистр сдвига может генерировать последовательность с периодом $3 = 2^2 - 1$. Трехразрядный регистр сдвига изображен на рис. 6.4*б* вместе с последовательностью, которую он генерирует. (Последовательность следует читать справа налево. Самый крайний символ справа был первым символом на выходе регистра.) Всегда, когда те же самые три символа встречаются второй раз, последовательность вновь начинает повторять себя, так как любые три последовательных символа определяют оставшуюся последовательность. Этот трехразрядный регистр сдвига генерирует последовательность с периодом $7 = 2^3 - 1$. Справедливо следующее утверждение: существует некоторое *линейное* устройство с обратной связью (т. е. такое, которое использует лишь суммирование по модулю два), с помощью которого k-зарядный регистр сдвига может генерировать двоичную последовательность с периодом 2^k-1 при любом целом k. Доказательство этого утверждения следует непосредственно из результатов, полученных в гл. 13, и здесь приведено не будет. Следует подчеркнуть, что не все линейные цепи с обратной связью порождают последовательности с периодом 2^k-1. На самом деле лишь малая доля возможных устройств с обратной связью приводит к желаемым результатам.

Последовательность с периодом 2^k-1, порождаемая линейным k-разрядным регистром сдвига, часто называется *последовательностью максимальной длины линейного регистра сдвига.* Основание для этого названия становится очевидным, если заметить, что период этой последовательности равен минимальному числу символов, отделяющих любые две одинаковые k-последовательности в ней. Это происходит потому, что содержимое k элементов памяти однозначно определяет последующий выход. Далее, если все элементы памяти содержали *нули* в какой-то момент, то выход будет *нулевым* все время, начиная с этого момента. Таким образом, самая длинная последовательность на выходе k-разрядного регистра сдвига может содержать каждую ненулевую k-последовательность один и только один раз до того момента, как она начнет повторять себя. Так как существует точно 2^k-1 таких (двоичных) k-последовательностей и так как любая последовательность с периодом N содержит N l-последовательностей для любого $l \leqslant N$, то период последовательности k-разрядного линейного регистра сдвига не может быть больше $N=2^k-1$.

Мы еще не показали, что желательные автокорреляционные свойства последовательности максимальной длины $\{1, 1, 0\}$ сохраняются в более длинных последовательностях. Это легко сделать, если учесть следующие два свойства последовательности максимальной длины линейного регистра сдвига:

1. Сумма по модулю два последовательности максимальной длины и последовательности, полученной путем любого циклического сдвига ее самой на любое число позиций l, где $l \neq 0$ по модулю N, является некоторой третьей последовательностью, полученной циклическим сдвигом той же самой последовательности.

2. Любая линейная последовательность максимальной длины 2^k-1 должна содержать 2^{k-1} *единиц* и $2^{k-1}-1$ *нулей.*

Докажем оба этих утверждения. Однако до этого рассмотрим их следствия, касающиеся автокорреляционной функции этих последовательностей.

Автокорреляционная функция временно́й функции $x(t)$, представляемой последовательностью *единиц* и *минус единиц,* как уже было отмечено, определяется ее значениями в точках $\tau_j = jT_0/N$. Если x_i является значением i-го элемента этой последовательности ($x_i=+1$ или $x_i=-1$), то

$$\rho_j = \rho\left(j\,\frac{T_0}{N}\right) = \frac{1}{N}\sum_{i=1}^{N} x_i x_{i+j} = \frac{A_j - D_j}{N}, \tag{6.81}$$

где $x_{N+l} \equiv x_l$ и A_j обозначает число случаев, когда $x_i = x_{i+j}$, а D_j — число случаев, когда $x_i \neq x_{i+j}$. Последнее выражение в правой части равенства (6.81) справедливо независимо от того, используется ли последовательность *единиц* и *минус единиц*, или *единиц* и *нулей*. Но число случаев, когда $x_i = x_{i+j}$ в последовательности *единиц* и *нулей* равно числу *нулей* в N-последовательности $\{x_i \oplus x_{i+j}\}$. Первое из двух свойств линейной последовательности максимальной длины, упомянутых выше, утверждает, что сумма последовательностей $\{x'_i = x_i \oplus x_{i+j}\}$, где $j \neq 0$ по модулю N является просто циклическим сдвигом последовательности $\{x_i\}$, $\{x'_i = x_{i+l}\}$ для некоторого целого l. Второе свойство, в свою очередь, утверждает, что число *нулей* в последовательности $\{x_{i+l}\}$, и, следовательно, в N-последовательности $\{x_i \oplus x_{i+j}\}$ равно $2^{k-1}-1$. Следовательно,

$$\rho_j = \frac{A_j - D_j}{N} = \frac{(2^{k-1}-1)-(2^{k-1})}{2^k - 1} = -\frac{1}{N} \tag{6.82}$$

для любого $j \neq 0$ по модулю N. Когда $j = 0$ по модулю N, то, конечно, $A_j = N$ и $\rho_j = 1$. Если эти два утверждения относительно линейных последовательностей максимальной длины справедливы (а они вскоре будут доказаны), то временна́я функция $x(t)$, соответствующая такой последовательности, имеет автокорреляционную функцию, график которой приведен на рис. 6.5. Таким образом, для коэффициентов корреляции $\rho_{\mu\nu} = \rho_{|\mu-\nu|} = -(1/N)$, $\mu \neq \nu$, и они подходят очень близко к нижней границе $-[1/(N-1)]$, как указывалось ранее. Фактически никакая двухуровневая последовательность длины N, большей двух, не может улучшить этот результат. Действительно, из ф-лы (6.81) имеем $\rho_j = l/N$, где l — некоторое целое число, а так как $\max\limits_j \rho_j \geqslant -[1/(N-1)]$, то $l \geqslant -[N/(N-1)]$. Но в силу того, что l — целое число, оно должно быть больше или равно -1 для всех $N > 2$.

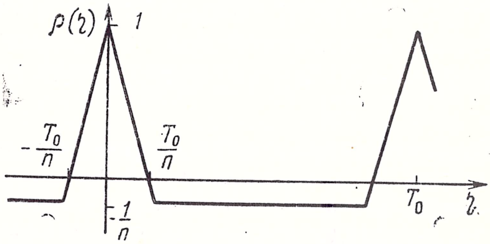


Рис. 6.5. Периодическая автокорреляционная функция последовательности максимальной длины

Докажем теперь оба утверждения, из которых следует справедливость равенства (6.82). Второе утверждение, что линейная последовательность максимальной длины 2^k-1 содержит $2^{k-1}-1$ *нулей* и 2^{k-1} *единиц*, следует почти непосредственно из сделанного ранее замечания, что каждая k-последовательность должна появляться один и только один раз в последовательности максимальной длины, имеющей длину 2^k-1. Каждый символ последовательности содержится точно в k последовательностях длины k (он является первым символом в одной, вторым символом в другой последовательности и т. д.). Поэтому число *единиц* в последовательности

$$M=\frac{1}{k}\sum_{i=1}^{2^k} m_i=\frac{1}{k}\left(2^k\,\frac{k}{2}\right)=2^{k-1}, \qquad (6.83)$$

где m_i — число *единиц* в i-й ненулевой k-последовательности. Число нулей, конечно, равно $2^k-1-M=2^{k-1}-1$.

Первое из этих двух утверждений (т. е. что последовательность $\{x_i\oplus x_{i+j}\}$ является последовательностью вида $\{x_{i+l}\}$ для некоторого целого l), необходимое, чтобы вычислить автокорреляционную функцию $x(t)$, является следствием линейности регистра сдвига, генерирующего эти последовательности. Любой элемент в последовательности является линейной комбинацией k предыдущих элементов

$$x_i=\sum_{\nu=1}^{k} a_\nu x_{i-\nu}, \qquad (6.84)$$

где суммирование проводится по модулю два. Коэффициенты a_ν равны либо *единице,* либо *нулю* и зависят от того, является ли выход соответствующего элемента памяти входом для сумматора по модулю два или нет. Сумма $x_i\oplus x_{i+j}$ может быть записана в виде

$$(x_i\oplus x_{i+j})=\sum_{\nu=1}^{k} a_\nu(x_{i-\nu}\oplus x_{i+j-\nu}). \qquad (6.85)$$

В соответствии с этим последовательность $\{x'_i=x_i\oplus x_{i+j}\}$ также может быть порождена той же самой логической цепью обратной связи, что и первоначальная последовательность $\{x_i\}$. Так как любая k-последовательность однозначно определяет остаток этой последовательности, то все ненулевые k-последовательности должны где-либо встречаться в ней, если встречается какая-либо из них. Последовательность либо содержит только *нули*, либо является некоторой циклической перестановкой любой другой последовательности максимальной длины, порождаемой с помощью той же самой логической цепи. Если две k-последовательности $x_i, x_{i+1}, \ldots, x_{i+k-1}$ и $x_{i+j}, x_{i+j+1}, \ldots, x_{i+j+k-1}$ не являются равными (а они равны только, если $j=0$ по модулю N), то последовательность, порождаемая их суммой, не является последовательностью одних *нулей*. Следовательно, кроме случая, когда $j=0$ по модулю N, сумма любых двух циклических перестановок одной и той же последовательности максимальной длины линейного регистра сдвига представляет собой третью перестановку той же самой последовательности, что и доказывает первое утверждение.

В силу того что эти последовательности имеют некоторые общие свойства со случайными двоичными последовательностями (ср. с гл. 13), они часто называются в литературе *псевдослучайными* или *псевдошумовыми* (ПШ) последовательностями. Последнее название будет использоваться в последующем изложении для обозначения последовательностей максимальной длины регистра сдвига. Следует отметить, что существуют также двоичные последовательности, отличные от псевдошумовых последовательностей и имеющие требуемые двухуровневые корреляционные функции. Хотя эти последовательности дополняют псевдошумовые последовательности (они могут иметь периоды, отличные от 2^k-1), они обычно более трудны для генерирования и поэтому используются не так часто.

Псевдошумовая последовательность дает метод реализации сигнала с эффективной длительностью импульса $\Delta T=T_0/N$ секунд (с $N=2^k-1$) и в то же время позволяет сохранить постоянной излучаемую мощность. Соответственно она может быть использована для целей синхронизации почти таким же образом, как прямоугольный импульс той же самой эффективной длительности. Рассмотрения § 6.3, в частности, касающиеся отслеживания периодического прямоугольного импульса с помощью системы ФАПЧ, в равной мере применимы к отслеживанию ПШ последовательностей. Если принимаемый сигнал представляет собой ПШ последовательность $Ap(t)$, то сигнал ошибки, дающий дисперсию фазовой ошибки (6.12) (с $\Delta t=\Delta T$), может быть реализован, например, с помощью использования местного (имеющего единичную мощность) сигнала $p^*(t)=\sqrt{N/2(N+1)}[p(t+\Delta T/2)-p(t-\Delta T/2)]$. Эффективная мощность сигнала в действительности больше в $(N+1)/N$ раз, чем в случае прямоугольного импульса длительности ΔT.

6.8. Выбор синхросигнала. Последовательности, быстро входящие в синхронизм

В предыдущих параграфах этой главы рассматривались оценки времени, необходимого для того, чтобы достичь требуемой точности временно́й синхронизации с помощью различных алгоритмов поиска и различных синхросигналов. Хотя выбор того или иного метода поиска или синхросигнала, или их обоих часто обусловливался внешними ограничениями, во многих случаях конструктор может обладать широкой свободой в выборе системы. При этом возникает вопрос о том, какой метод синхронизации является оптимальным (в смысле минимума времени поиска) при этих ослабленных ограничениях.

Если нет никаких ограничений вообще (кроме обычных ограничений на мощность), то оптимальный метод состоит, очевидно, в передаче псевдошумовой последовательности (или ее эквивалента) по синхроканалу и в принятии решения максимального правдоподобия относительно правильной метки (ср. с § 4.2).

Как уже было отмечено, одно из наиболее частых ограничений — ограничение на сложность устройств, приводящее к тому, что метки должны рассматриваться поочередно, а не одновременно. Каков наилучший класс сигналов для использования в этом случае? По очевидным соображениям в этом случае также часто используются псевдошумовые последовательности. Действительно, как показывает беглый просмотр предыдущих параграфов этой главы, процедуры поиска наиболее эффективны, когда $\rho = -1/N$ (или в некогеретном случае, когда $\rho = 0$). Если используется псевдошумовая последовательность, условия, приведенные в § 2.7, удовлетворяются, и *оптимальный* поочередный поиск является последовательным поиском с $\alpha \to 1$. Поэтому минимально возможное математическое ожидание времени поиска, которое можно получить с помощью ПШ последовательности, прямо пропорционально длине последовательности [ср. с (6.45) при $n = N$].

Есть основания полагать, что время поочередного поиска могло бы быть намного медленнее возрастающей функцией N. К этому заключению приводят довольно очевидные недостатки процедуры поочередного поиска, когда используются псевдошумовые последовательности. Независимо от используемого алгоритма, когда N велико, значительно большее время тратится на отвержение ошибочных меток, чем на принятие правильной метки. Вместе с тем отвержение устраняет лишь одну метку среди конкурирующих, в то время как принятие устраняет $N-1$ меток. Плоды непропорциональны усилиям. Метод оценивания меток, предложенный в § 6.5, обходит эту трудность. Наблюдение дает одно и то же количество информации независимо от того, какая из меток рассматривается на самом деле. Хотя требуемое для принятия решения время при использовании этого метода больше, чем математическое ожидание времени поиска при последовательном методе, по крайней мере, если синхросигнал является псевдошумовой последовательностью, алгоритм оценивания в некотором смысле является более эффективным.

Способом уменьшения времени поиска является использование такого алгоритма оценивания меток совместно с алгоритмом, который выделяет одно и то же количество информации из каждого наблюдения с помощью эффективного при этом алгоритме класса сигналов. Предположим, что синхросигнал таков, что наблюдаемые, относящиеся к какой-либо частной метке, принимают в отсутствие шума одно из m возможных значений в зависимости от того, какая метка является правильной. Если m равно N и каждое возможное соотношение между правильной и наблюдаемой метками приводит к единственному ожидаемому значению наблюдаемой, то поиск заканчивается после принятия одного единственного решения. Если $m = N^{1/2}$, то необходимы два таких решения. В общем случае для любого значения m вплоть до m^r различных меток могут быть разрешены с помощью r решений. Поэтому в идеале r может быть таким же малым, как наименьшее целое число, равное или большее $\log_m N$.

Для того чтобы минимизировать число необходимых решений, m должно быть, по возможности, большим. Вместе с тем дисперсия величины решающей переменной должна быть обратно пропорциональна квадрату числа уровней, которые нужно различить, если требуется принять надежное решение. В соответствии с этим время, необходимое для принятия решения, грубо, должно быть, пропорционально m^2, а полное время поиска пропорционально $m^2 \log_m N = (m^2/\log_e m) \log_e N$. Дифференцируя выражение $m^2/\log_e m$ по m, находим, что оно является возрастающей функцией m при $m > e^{1/2}$ и убывающей функцией при $m < e^{1/2}$. Так как m должно быть целым, его оптимальное значение приближенно равно 2.

Таким образом, поиск должен производиться на основе двоичного решения относительно каждой метки, так же как в большинстве процедур поиска, описанных ранее, но с одним важным отличием. Каждое двоичное решение должно устранять половину меток, все еще конкурирующих на этом этапе поиска, независимо от того, какая метка рассматривается. Если это можно сделать, полное время поиска будет пропорционально $\log_2 N$, а не N, что дает значительный выигрыш, когда N велико.

Легко выбрать такой сигнал, чтобы первое двоичное решение устранило половину конкурирующих меток. Предположим, в частности, что синхросигналы $s_1(t)$ являются синусоидами с единичной **мощностью** или прямоугольными функциями с периодом $2T_0/N$. Подойдет также любая функция времени $f(t)$, имеющая минимальный период $2T_0/N$ и удовлетворяющая условию $f[t + (T_0/N)] = -f(t)$, т. е. любая *антипериодическая* функция. Коэффициенты автокорреляции $\rho(\tau = iT_0/N) \overset{\Delta}{=} \rho_i$ такого сигнала имеют вид

$$\rho_i = (-1)^i. \tag{6.86}$$

Решение максимального правдоподобия относительно того, является ли номер наблюдаемой метки четным или нечетным (относительно правильной метки), принимается на основе использования суммы интегралов вида

$$z_1(j) = \int_{jT_0}^{(j+1)T_0} y_1(t)\, s_1(t)\, dt, \tag{6.87}$$

где принимаемый сигнал $y_1(t)$ равен $As_1[t - (iT_0/N)] + n(t)$ для некоторого целого i. Если сумма $\sum\limits_{j=0}^{M-1} z_1(j)$ положительна, то проверяемая и правильная метки, по-видимому, имеют одинаковую четность (т. е. они разделены нечетным числом меток); если эта сумма отрицательна, они должны иметь разную четность. В любом случае, в соответствии с нашим желанием, после решения будут оставаться лишь $N/2$ конкурирующих меток.

Но после того как это решение будет принято, ситуация изменится только в том, что останутся лишь $N/2$ равномерно расположенных меток, а не N меток, как первоначально. Таким образом, второй синхроканал мог бы быть использован в точности таким же образом, как первый канал, для того чтобы вновь снизить вдвое число конкурирующих меток. Нужно лишь передать по этому второму каналу антипериодический сигнал $s_2(t)$ с периодом $2T_0/N$ и принять решение на основе интегралов вида

$$z_2(t) = \int_{jT_0}^{(j+1)T_0} y_2(t)\, s_2(t)\, dt. \tag{6.88}$$

И в общем случае, если N — степень числа 2, то число конкурирующих меток может быть снижено от $N/2^{i-1}$ до $N/2^i$ с помощью передачи по i-му каналу антипериодического сигнала $s_i(t)$ с периодом $2^i T_0/N$ и образования интегралов

$$z_i(j) = \int_{jT_0}^{(j+1)T_0} y_i(t)\, s_i(t)\, dt. \tag{6.89}$$

Требуется лишь $\log_2 N$ таких каналов и, следовательно, $\log_2 N$ таких решений для того, чтобы определить правильную метку (в предположении, что все решения делаются правильно).

Хотя эта процедура описана так, словно в распоряжении имеются $\log_2 N$ раздельных синхроканалов, в действительности нужен лишь один канал. Это происходит потому, что сигналы $s_i(t)$ являются ортогональными:

$$\frac{1}{T_0}\int_0^{T_0} s_\nu(t)\, s_\mu(t)\, dt = 0; \quad \mu \neq \nu. \tag{6.90}$$

Таким образом, передаваемый сигнал может иметь вид

$$s(t) = \frac{1}{\sqrt{\log_2 N}} \sum_{i=1}^{\log_2 N} s_i(t), \tag{6.91}$$

а каждая решающая переменная $z_i(j)$ может быть сформирована так, что на нее не будет влиять присутствие любых других сигналов $s_l(t)$, $l \neq i$. Если амплитуда каждого из составляющих сигналов $s_i(t)$ равна $1/\sqrt{\log_2 N}$, как указывает равенство (6.91), то полная мощность принимаемого сигнала не зависит от N.

Тогда на i-м этапе поиска решение должно строиться на основе статистик $z_i(j)$ относительно того, сравнимы ли по модулю 2^i метка принимаемого сигнала и метка сигнала $s_i(t)$ (гипотеза H_i) или они не сравнимы (гипотеза $\overline{H}_i$). Так как оба рода ошибок равноценны, если рассматривать их действие на результат поиска, то соответствующие вероятности ошибок α и β должны быть равны. Оптимальное в смысле минимума математического ожидания требуемого времени решение на каждом этапе, конечно, будет последовательным решением. Математическое ожидание числа требующихся наблюдаемых, в силу того что $\alpha = \beta$, равно

$$E(M \mid H_i) = E(M \mid \overline{H}_i) = \frac{(1-2\alpha)\log_e \dfrac{1-\alpha}{\alpha}}{E(\zeta_i \mid H_i)}, \tag{6.92}$$

где ζ_i — логарифм отношения плотностей вероятностей

$$\frac{p_0(z_i)}{p_1(z_i)} = \exp\left\{\frac{2\eta}{\sigma^2} z_i\right\}; \tag{6.93}$$

$\eta \underline{\Delta} \, |E(z_i)| = AT_0/\sqrt{n}$; $\sigma^2 \underline{\Delta} \, \mathrm{var}(z_i) = N_0T_0/2$ и $n \underline{\Delta} \log_2 N$. Таким образом, математическое ожидание времени поиска равно $\overline{M}_T T_0$ секунд, где

$$\overline{M}_T = (\log_2 N)\, E(M \mid H_i) = \frac{1-2\alpha}{4R} \log_e\left(\frac{1-\alpha}{\alpha}\right)(\log_2 N)^2 \tag{6.94}$$

с $R = A^2T_0/N_0$. Наконец, так как вероятность принятия ошибочной метки P_e приближенно равна $n\alpha$, когда $n\alpha \ll 1$ [ср. с § 2.6; $n\alpha\{1 - [(n-1)/2]\alpha\} \leqslant P_e = 1 - (1-\alpha)^n \leqslant n\alpha$], то получаем

$$\overline{M}_T \approx \frac{1}{4} \log_e\left(\frac{\log_2 N}{P_e}\right) \frac{(\log_2 N)^2}{R}. \tag{6.95}$$

Можно было бы также на каждом этапе производить решение с фиксированным объемом выборки. Получающееся в результате время поиска, когда вероятность P_e мала, приближенно в четыре раза больше, чем время последовательного поиска в тех же самых условиях.

Хотя результат (6.95) в некотором отношении хуже, чем пропорциональность первой степени величины $\log_2 N$, на которую было указано в предыдущих абзацах[1]), он тем не менее дает значительное снижение времени поиска по сравнению с временем, которое требуется при использовании псевдошумовых последовательностей. Более того, кажется очевидным, что при поочередном поиске никакое дальнейшее снижение невозможно, по крайней мере, если решения должны быть двоичными. Сигнал, использованный в каждом «канале», был оптимальным в том смысле, что никакой другой сигнал с той же самой энергией не мог бы сделать эти две возможные гипотезы более различимыми. Так как каждое решение было одинаково важно для окончательного результата, то все «каналы» должны иметь одну и ту же энергию, как в действительности и было. Никакая процедура решения не является, в среднем, более быстрой, чем последовательное решение, так что время, затраченное на каждое решение, минимально. И, наконец, в среднем, правильную метку могут определить не менее чем $\log_2 N$ двоичных решений.

Недостаток этих сигналов по сравнению с псевдошумовыми последовательностями состоит в непостоянстве передаваемой мощности. Пиковая мощность [см. (6.91)] в $\log_2 N$ раз больше средней мощности. Хотя это отношение значительно лучше по сравнению с отношением $N/1$, характерном для импульсного сигнала длительности T_0/N, все же использование таких сигналов может оказаться неудобным. В любом случае эти сигналы могут быть заменены двоичными последовательностями постоянной мощности лишь с минимальным ухудшением характеристик.

---

[1]) Заметим, что если можно изменять передаваемый сигнал в подходящие моменты времени в течение процесса синхронизационного поиска, то сигналы $s_i(t)$ могут передаваться поочередно. Мощность каждого составляющего сигнала можно было бы при этом эффективно увеличить в $\log_2 N$ раз, и время поиска стало бы, на самом деле, пропорциональным $\log_2 N$. *(Прим. авт.)*.

Чтобы показать, как это можно сделать, предположим, что сигналы $s_i(t)$ прямоугольны, и заметим, что они могут быть однозначно представлены последовательностью $s_i=(\sigma^i{}_1, \sigma^i{}_2, \ldots, \sigma^i{}_N)$ *единиц* и *минус единиц*; $\sigma^i{}_j$ соответствует амплитуде сигнала $s_i(t)$ на интервале $(j-1)T_0/N<t<jT_0/N$. При этом сигнал $s(t)$ представляется последовательностью

$$s=\left(\sum_{i=1}^{n}\sigma_1^i,\ \sum_{i=1}^{n}\sigma_2^i,\ \ldots,\ \sum_{i=1}^{n}\sigma_N^i\right). \tag{6.96}$$

Цель состоит в том, чтобы заменить эту последовательность последовательностью $s'=(\theta_1, \theta_2, \ldots, \theta_N)$ *единиц* и *минус единиц*, соответствующей сигналу $s'(t)$ таким образом, чтобы минимизировать увеличение математического ожидания времени синхронизационного поиска. Согласно (6.94), это время поиска определяется лишь величинами η и σ, где σ не зависит от принимаемого сигнала. Таким образом, выберем s' так, чтобы максимизировать величину

$$\eta_i'=A\int_0^{T_0}s'(t)\,s_i(t)\,dt=\frac{AT_0}{N}\sum_{j=1}^{N}\theta_j\sigma_j^i$$

для всех $i=1, 2, \ldots, n=\log_2 N$. Но

$$\min_i \eta_i' \leqslant \operatorname*{ave}_i \eta_i'=\frac{AT_0}{Nn}\sum_{i=1}^{n}\sum_{j=1}^{N}\theta_j\sigma_j^i=\frac{AT_0}{Nn}\sum_{j=1}^{N}\theta_j\sum_{i=1}^{n}\sigma_j^i\leqslant\frac{AT_0}{Nn}\sum_{j=1}^{N}\left|\sum_i\sigma_j^i\right|,$$

(6.97

где последнее неравенство переходит в равенство тогда и только тогда, когда

$$\theta_j=\operatorname{sgn}\left\{\sum_i\sigma_j^i\right\}\triangleq\begin{cases}1, & \sum\limits_i\sigma_j^i\geqslant 0;\\ -1, & \sum\limits_i\sigma_j^i<0.\end{cases} \tag{6.98}$$

Определение функции $\operatorname{sgn}\{x\}$ при $x=0$ несущественно при рассмотрении этого последнего утверждения. Для удобства определим $\operatorname{sgn}\{0\}=1$, хотя это расходится с обычным определением, при котором $\operatorname{sgn}\{0\}=0$. Как будет показано, если θ_j определяется равенством (6.98), величины $\min\eta'_i$ и $\operatorname{ave}\eta'_i$ достигают верхней границы в (6.97). Таким образом, последовательность s', которая называется *последовательностью, быстро входящей в синхронизм*, является оптимальной в тех условиях, которые здесь рассматриваются. Последовательность, быстро входящая в синхронизм, s'

длины $N=32$ изображена на рис. 6.6 вместе с составляющими последовательностями s_i.

Для доказательства оптимальности последовательности s' заметим, что множество n-последовательностей $\{\sigma^1{}_j, \sigma^2{}_j, \ldots, \sigma^n{}_j\}$ содержит каждую из N двоичных n-последовательностей (*единиц* и

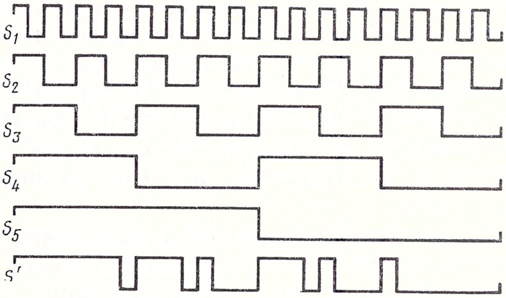


Рис. 6.6. Последовательность, быстро входящая в синхронизм, и ее компоненты ($N=32$)

минус единиц) один и только один раз. Более того, так как θ_j — симметричная функция $\sigma^i{}_j$ и $\sigma^k{}_j$, то

$$\eta'_k - \eta'_i = \frac{AT_0}{N} \sum_{j=1}^{N} (\sigma^k_j - \sigma^i_j)\,\theta_i = \frac{AT_0}{N} \sum_{j=1}^{N} (\sigma^i_j - \sigma^k_j)\,\theta_j = \eta'_i - \eta'_k$$

и, следовательно, $\eta'_i = \eta'_k$ для всех i и k. В соответствии с этим $\operatorname{ave} \eta'_i = \min\limits_i \eta'_i$, и все неравенства в (6.97) в действительности являются равенствами, если θ_j определяется так, как указано выше. Наконец,

$$\eta' \triangleq \eta'_i = \frac{AT_0}{Nn} \sum_{j=1}^{N} \left| \sum_{i=1}^{n} \sigma^i_j \right| = \frac{2AT_0}{Nn} \sum_{\nu=0}^{[n/2]} \binom{n}{\nu} (n - 2\nu) =$$

$$= \begin{cases} \dfrac{AT_0}{2^{n-1}} \dbinom{n-1}{\frac{n-1}{2}}, & n \text{ нечетное;} \\ \dfrac{AT_0}{2^n} \dbinom{n}{\frac{n}{2}}, & n \text{ четное,} \end{cases} \tag{6.99}$$

где квадратные скобки обозначают целую часть находящейся в ней дроби. Последняя сумма опять вычисляется с учетом того, что каждая из N двоичных n-последовательностей появляется точно один раз в множестве $\{\sigma^1{}_j, \sigma^2{}_j, \ldots, \sigma^n{}_j\}$.

Когда n велико, применение приближения Стирлинга для биномиальных коэффициентов дает

$$\eta' \approx \sqrt{\frac{2}{\pi}} \frac{AT_0}{(\log_2 N)^{1/2}}. \tag{6.100}$$

Единственной платой за замену передаваемого сигнала $s(t)$ на $s'(t)$ является увеличение времени поиска приближенно в $\pi/2$ раз [см. ф-лу (6.94), где нужно η заменить на η'].

Интересно отметить, что последовательности, быстро входящие в синхронизм, содержат свой собственный отсчет времени. А именно, если такая последовательность подается на вход системы ФАПЧ, если местный сигнал $z(t)$ является прямоугольным, с периодом, равным периоду наиболее высокочастотной компоненты, определяющей последовательность, и если ширина полосы цепи порядка $1/2T_0$ или меньше, то эта компонента будет отслежена. Для системы последовательность оказывается чисто прямоугольной функцией с амплитудой $A\eta'$, где η' определяется ф-лой (6.99). Ошибка отслеживания поэтому равна $\sigma_\Phi^2 = (\pi/2)^2 (N_0 BL/A^2(\eta')^2)$ (см. § 6.3).

Обычно значительно большую мощность следует придать компоненте, по которой производится отсчет времени, а не каким-либо другим компонентам, определяющим составную последовательность, так как временнáя компонента определяет окончательную точность синхронизации. Это можно выполнить с помощью простого увеличения веса наивысшей частоты последовательности при определении составной последовательности. Таким образом, например, когда $N=16$, можно так выбрать знаки сумм соответствующих элементов в четырех последовательностях

$$\begin{array}{cccccccccccccccc}
2 & -2 & 2 & -2 & 2 & -2 & 2 & -2 & 2 & -2 & 2 & -2 & 2 & -2 & 2 & -2 \\
1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\
1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1,
\end{array}$$

чтобы получить составную последовательность

$$\begin{array}{cccccccccccccccc}
1 & 1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & -1 & -1.
\end{array}$$

Эта последовательность имеет корреляцию $\eta_{cl}=3/4$ с временнóй компонентой и $\eta=1/4$ с каждой из остальных компонент последовательности. В общем случае, если отсчет времени представляется последовательностью $a, -a, a, -a, \ldots$, а другие компоненты представляются последовательностями $+1$ и -1, корреляция между составной последовательностью, сформированной таким образом, и временнóй компонентой, как легко видеть, будет равна

$$\eta_{cl} = (2A - N)/N, \qquad (6.101)$$

где $A = 2 \sum_{i=0}^{[(n-1+a)/2]} \binom{n-1}{i} - \binom{n-1}{\frac{n-1+a}{2}}$, а $n = \log_2 N$. Второй биномиальный коэффициент берется равным нулю, если $(n-1+a)/2$ — не целое число. Аналогично корреляция с каждой из остальных компонент последовательности равна

$$\eta = (2B - N)/N, \qquad (6.102)$$

где

$$B = 2\sum_{i=0}^{[(n-1+a)/2]} \binom{n-2}{i} - \binom{n-2}{\frac{n-1+a}{2}} + 2\sum_{i=0}^{[(n-1-a)/2]} \binom{n-2}{i} - \binom{n-2}{\frac{n-1-a}{2}}.$$

Заметим, что $\eta_{cl}=1$, $\eta=0$, когда $a>n-1$, и что $\eta_{cl}=\eta$, когда $a=1$. Если n относительно велико, то можно получить почти любое требуемое соотношение между η_{cl} и η при некотором a из интервала $1 \leqslant a \leqslant n-1$.

6.9. Заключительные замечания

Эта глава посвящена методам установления синхронизации, выбору сигнала для синхронизации и методам эффективной его обработки, когда имеется отдельный канал, используемый исключительно для этой цели. Следует заметить, что наличие отдельного канала не обязательно требует отдельных передатчика и приемника. Синхросигнал может быть различными способами уплотнен с сигналами, переносящими информацию, например, с помощью использования раздельных поднесущих или чередования двух сигналов во времени. В некоторых случаях система связи может работать в двух режимах; исходный режим установления синхронизации необходим для следующего режима передачи. Синхронизация поддерживается либо с помощью постоянного отслеживания отсчетов времени, либо она основывается на достаточной стабильности генераторов в передатчике и в приемнике. Независимо от используемой схемы уплотнения результаты этой главы могут быть применены в случае, если синхроканал можно рассматривать как совершенно отдельный.

Хотя это не всегда так, первым шагом в процессе синхронизации, вообще говоря, является установление общего отсчета времени во всей системе связи. Это приводит к передаче периодического сигнала и отслеживанию его фазы в приемнике. Если период этого сигнала времени равен (или больше) минимальному приемлемому синхронизационному интервалу неоднозначности T_0 секунд, то дальнейшие операции не нужны. Однако, если в целях снижения времени входа в синхронизм используется сигнал времени с периодом $\Delta T < T_0$, то остаются $N = T_0/\Delta T$ не определенных синхронизационных меток и сигнал должен устранить эту N-кратную неоднозначность.

Оптимальная стратегия для устранения неоднозначности зависит от используемого для этой цели сигнала и ограничений на сложность оборудования. Главные выводы по этому вопросу можно сформулировать следующим образом:

1. Если нет ограничений на сложность оборудования, а также форму синхросигнала, кроме, возможно, ограничения на пиковую мощность, то оптимальным является псевдошумовой сигнал или эквивалентный ему (периодический ортогональный сигнал для некогерентного канала), а оптимальным приемником являются параллельно соединенные согласованные фильтры, по одному для каждой из меток сигнала. Время решения пропорционально тогда $\log N$, где N — число конкурирующих меток сигнала.

2. Если ограничения на сложность оборудования заставляют производить поочередные наблюдения меток, то оптимальным является сигнал, который рассматривался в § 6.8. Если существует жесткое ограничение пиковой мощности, то эти последовательности могут быть превращены в двоичные последовательности, быстро входящие в синхронизм, что приведет лишь к незначительному увеличению времени поиска. В любом случае время поиска будет порядка $(\log N)^2$. Если в этих условиях используются псевдошумовые последовательности, то время поиска будет порядка N. (Существуют методы объединения нескольких псевдошумовых последовательностей для получения составного сигнала. Время поиска при использовании таких последовательностей меньше, чем при использовании только ПШ последовательности с одной компонентой, но больше, чем для последовательностей, быстро входящих в синхронизм.)

3. Если имеются также ограничения на форму синхросигнала, то оптимальным алгоритмом поиска может быть либо задержанное решение при последовательном поиске, либо оценивание, зависящее от конкретного вида используемого сигнала. В любом случае время поиска будет, как правило, пропорционально N^2.

4. Если жесткие ограничения на оборудование запрещают использование всех алгоритмов поиска, кроме простейшего, (т. е. последовательного поиска с фиксированным объемом выборки), то время поиска может оказаться пропорциональным N^3.

В той части выводов, которые относились к построению сигнала, молчаливо предполагалось, что синхронизационный канал имеет ограничение на отношение сигнал/шум, а не на ширину полосы. На самом же деле, если произведение длительности импульса на ширину полосы порядка 3 или 4, или выше, то можно полностью пренебречь ограничением на ширину, и выводы, относящиеся к построению сигнала, не нуждаются в корректировке. Однако, если есть ограничения на ширину полосы, может оказаться, что невыгодно делать длительность импульса такой малой, какой она должна была бы быть при наличии лишь ограничений на отношение сигнал/шум. Тем не менее возможно с помощью изменения формы импульса сузить *эффективную* длительность импульса, не нарушая ограничений на полосу канала. Наиболее эффективная форма импульса определяется полосовыми характеристиками канала, и трудно получить какие-либо общие выводы в этом направлении. Те же оговорки можно сделать относительно выбора частоты синусоидальной поднесущей, используемой для отсчета времени. Очевидно, сигнал времени должен находиться в пределах полосы пропускания канала, и это может привести к тому, что его частота окажется меньше, чем та, которая предлагается в § 6.2.

Следует также отметить второе предположение, которое лежит в основе приведенных выше выводов. А именно, предполагалось, что корреляции, дающие решающие переменные, вычисляются за некоторое целое число периодов сигнала синхронизации. Если отношение сигнал/шум и период сигнала синхронизации достаточно велики, то можно принять надежное решение относительно фазы сигнала еще до завершения наблюдения полного периода. В этом случае приведенные выше результаты перестают быть справедливыми. *Коэффициенты частичной корреляции,* получаемые путем вычисления взаимной корреляции псевдошумовой последовательности и ее местного варианта или последовательности, быстро входящей в синхронизм, и одной из компонент этой последовательности лишь на части этого периода, будут иметь ненулевые дисперсии даже в отсутствие шума. Псевдошумовые последовательности будут в этом случае лучше последовательностей, быстро входящих в синхронизм, и, если отношение сигнал/шум достаточно велико для того, чтобы оправдать использование частичных корреляций, будут несомненно работать лучше них. Один из методов использования этой возможности указан в задаче 6.6.

В этой главе рассматривалось оптимальное решение задачи наиболее эффективного использования имеющейся в распоряжении мощности сигнала. Так же, как и в предыдущих главах, обобщение исследований этой главы на ситуации, в которых рекомендации по достижению оптимума могут быть выполнены лишь приближенно, вообще говоря, является простым.

Что касается сложности оборудования, то наиболее уязвимым элементом в аппаратуре, которая необходима для реализации методов этой главы, несомненно является цепь отслеживания. На самом деле, синхронизация, очевидно, возможна без таких устройств, хотя их устранение, вообще говоря, весьма существенно скажется на мощности сигнала, необходимого для получения заранее заданной точности.

Если принимаемым сигналом является синусоида, то система ФАПЧ работает как узкополосный фильтр. Так как система способна отслеживать частоту сигнала, ее ширина полосы B_L может быть намного у́же, чем динамический частотный диапазон Δf принимаемого сигнала. Тем не менее принимаемый сигнал мог бы быть отфильтрован пассивным фильтром, имеющим ширину полосы частот $B \geqslant \Delta f$. Отфильтрованный сигнал тогда имел бы вид (ср. с § 5.4)

$$y_f(t) = A\sin(\omega_c t + \Phi) + n_f(t) = [A + n_1(t)]\sin(\omega_c t + \Phi) +$$

$$+ n_2(t)\cos(\omega_c t + \Phi) \approx A\sin\left(\omega_c t + \Phi + \frac{n_2(t)}{A}\right). \qquad (6.103)$$

Приближенное равенство имеет место тогда, когда $|n_f(t)| \ll A$, как и должно быть для того, чтобы извлеченный сигнал давал приемлемый отсчет времени. Таким образом, дисперсия фазовой ошибки приближенно равна

$$\sigma_\Phi^2 = \frac{E\left[n_2^2(t)\right]}{A^2} = \frac{N_0 B}{A^2}, \qquad (6.104)$$

где N_0 — спектральная плотность шума. Для того чтобы получить с фильтром, имеющим ширину полосы B, ту же самую точность, что и при работе с системой ФАПЧ с шириной полосы B_L, необходимо увеличить мощность сигнала в B/B_L раз. Так как $B \geqslant \Delta f$, в то время как, обычно, $B_L \ll \Delta f$, то требуемое увеличение мощности может быть ощутимым.

Тот же общий вывод относительно влияния устранения цепи отслеживания остается справедливым и для случая, когда принимаемый сигнал является несинусоидальным. Например, если сигнал синхронизации состоит из периодически передаваемых коротких импульсов, цепь отслеживания, описанная в § 6.3, иногда заменяется фильтром и следующим за ним пороговым устройством; оцениваемая метка определяется моментом, в который выход фильтра превышает некоторый порог[1]. Вновь ценой устранения цепи является значительное увеличение полосы частот синхронизатора (ср. с задачей 6.3) и, следовательно, соответствующее увеличение мощности сигнала, необходимой для получения удовлетворительных результатов.

Задачи

6.1. а) Сигнал $x(t-\tau)$ принимается в присутствии аддитивного белого гауссовского шума, имеющего одностороннюю спектральную плотность N_0. Функция $x(t)$ известна, но время задержки τ является случайной величиной, равномерно распределенной на интервале $(-T_0/2,\ T_0/2)$. Показать, что независимо от метода, используемого для оценки τ, среднеквадратическая ошибка оценивания ограничена снизу неравенством

$$\sigma_\tau^2 \geqslant \max_{0 \leqslant v \leqslant T_0/2} \frac{u^2}{8}\left\{1 - \operatorname{erf}\left[\frac{(1-\rho(u))\,R}{2}\right]^{1/2}\right\},$$

где $R = \mathscr{E}/N_0;\ \mathscr{E} = \int\limits_{-\infty}^{\infty} x^2(t)\,dt$ и $\rho(u) = 1/\mathscr{E}\left(\int\limits_{-\infty}^{\infty} x(t)\,x(t+u)\,dt\right)$.

Указание. Рассмотрите следующую задачу. Принимается один из двух равновероятных сигналов: $x_1(t) = x[t-(u/2)]$ и $x_2(t) = x[t+(u/2)]$. Для того чтобы определить, какой именно, оценивается время задержки сигнала τ и решение строится с использованием знака этой оценки $\hat{\tau}$. Очевидно, вероятность ошибочного решения

$$P_e = \frac{1}{2}\Pr\left\{\tau_e > \frac{u}{2}\,\middle|\,x_1\right\} + \frac{1}{2}\Pr\left\{\tau_e < -\frac{u}{2}\,\middle|\,x_2\right\},$$

---

[1] Задача синхронизации в этом виде тесно связана с задачей оценки времени задержки радиолокационного импульса при измерении расстояния. *(Прим. авт.).*

где $\tau_e=\tau-\hat{\tau}$ — ошибка оценивания. Получите сформулированный результат, используя ф-лы (4.12) и (4.13) для того, чтобы оценить снизу P_e и неравенство Чебышева $\Pr\{|x|\geqslant k\}\leqslant E(x^2)/k^2$ для того, чтобы провести дальнейшую оценку снизу.

б) Показать, что если

$$x(t)=\begin{cases}\left(\dfrac{\mathscr{E}}{\Delta T}\right)^{1/2} & \text{при } 0<t<\Delta T;\\ 0 & \text{в остальных случаях,}\end{cases}$$

то $\sigma_\tau^2\geqslant k(\Delta T)^2/R^2$, где $k=\max\limits_{0\leqslant\xi^2\leqslant R/2}\left[\dfrac{\xi^4}{2}(1-\operatorname{erf}\xi)\right]=0{,}0925.$

Сравните эту дисперсию ошибки оценивания с той, которая получается, когда тот же сигнал передается с периодом T_0 и его отслеживание производится системой ФАПЧ с шириной полосы $B_e=1/2T_0$ (ср. с § 6.3).

6.2. *Корень квадратный из среднеквадратической ширины полосы* B_0 периодической последовательности импульсов $x(t)$ определяется равенством

$$B_0^2=\frac{\int\limits_{-\infty}^{\infty}(\omega/2\pi)^2\,|X(\omega)|^2\,d\omega}{\int\limits_{-\infty}^{\infty}|X(\omega)|^2\,d\omega},$$

где $X(\omega)$ — преобразование Фурье $x(t)$.

а) Покажите, что если такая последовательность импульсов должна быть отслежена системой ФАПЧ, рассмотренной в § 6.3, то приближенное выражение для дисперсии фазовой ошибки при достаточно больших отношениях сигнал/шум имеет вид: $\sigma_\Phi^2=N_0B_L/A^2B_0^2T^2$, где T — период импульсной последовательности; A^2 — мощность принимаемого сигнала; N_0 — спектральная плотность шума; B_L — ширина полосы системы и B_0 — (конечная) определенная выше ширина полосы.

б) Используя неравенство Крамера—Рао, определите нижнюю границу дисперсии любой несмещенной оценки фазы такого сигнала и сравните с предыдущим результатом.

в) Покажите, что метод оптимизации длительности импульса, рассмотренный в § 6.3, в равной мере применим к импульсам, имеющим конечные ширины полос B_0, и приводит, по существу, к тем же самым результатам.

6.3. Одним из распространенных методов установления синхронизации является передача периодической последовательности коротких импульсов и установления моментов, в которые амплитуда соответствующим образом профильтрованного принимаемого сигнала превышает некоторый порог. Показать, что при достаточно больших отношениях сигнал/шум среднеквадратическая ошибка синхронизации будет равна ошибке при отслеживании того же сигнала системой ФАПЧ, имеющей ширину полосы $B_L=1/2T$ при частоте повторения импульсов $1/T$. Показать, что это справедливо для прямоугольных импульсов и для импульсов, имеющих конечную ширину полосы B_0, определенную в задаче 6.2.

Указание. При больших отношениях сигнал/шум соотношение между корнем квадратным из среднеквадратического значения временной ошибки σ_τ и корнем квадратным из среднеквадратического значения шума σ_n на выходе фильтра может быть аппроксимировано так, как показано на рис. 6.7.

Что является здесь аналогом вероятности потери синхронизации в системах ФАПЧ?

6.4. Фаза искаженного белым гауссовским шумом прямоугольного сигнала с периодом T должна быть оценена с помощью вычисления его корреляции одновременно с двумя прямоугольными сигналами, генерируемыми местным генератором и имеющими тот же самый период; один из этих местных сигналов задержан на время $T/4$ относительно другого. При условии, что после вычисления корреляции за MT секунд нормированный выход одного коррелятора равен x, а другого — y; показать, что формула оценки максимального правдоподобия времени задержки принимаемого прямоугольного сигнала имеет вид:

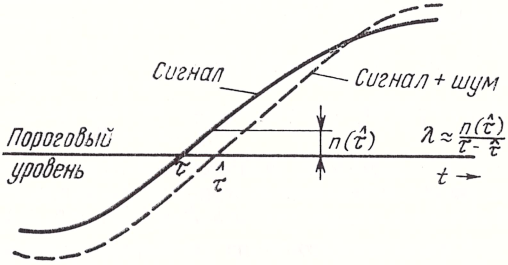


Рис. 6.7. Приближенное соотношение между уровнем шума и временно́й ошибкой

$$\hat{\tau} = \frac{T}{8}\,[2\operatorname{sgn} y - \operatorname{sgn} x \operatorname{sgn} y - \operatorname{sat}(x \operatorname{sgn} y - y \operatorname{sgn} x)],$$

где

$$\operatorname{sat} u = \begin{cases} u, & |u| < 1; \\ \operatorname{sgn} u, & |u| \geqslant 1 \end{cases} \quad \text{и} \quad \operatorname{sgn} u = \begin{cases} 1, & u \geqslant 0; \\ -1, & u < 0. \end{cases}$$

Указание. Положите $u=(x-y)/\sqrt{2}$, $v=(x+y)/\sqrt{2}$ и заметьте, что оценка максимального правдоподобия минимизирует величину $\{[x-E(x|\hat{\tau})]^2+[y-E(y|\hat{\tau})]^2\}^{1/2}$.

Определить среднеквадратическую ошибку этой оценки, когда отношение сигнал/шум велико. Сравнить ее с соответствующим параметром, относящимся к случаю, когда в качестве местного сигнала используется синусоида, а не прямоугольный сигнал.

6.5. Предположим, что синхросигнал является частотномодулированной несущей, т. е. предположим, что принимаемый сигнал имеет вид $\sqrt{2}A\sin[\omega_c t+\Delta f\times\int s(t)dt]+n(t)$, где $n(t)$ — широкополосный гауссовский шум. Хорошо известно и легко доказывается, что при отношениях сигнал/шум, превышающих порог ЧМ демодулятора, выход демодулятора имеет вид: $\Delta f s(t)+n'(t)/A$, где $n'(t)$ — производная $n(t)$. Этот сигнал должен быть отслежен системой ФАПЧ с фиксированной шириной полосы B_L, узкой по сравнению с Δf. Показать, что справедливы следующие утверждения:

а) Если $s(t)$ — синусоида, то достижимая точность синхронизации не зависит от ее частоты. (Это утверждение, конечно, справедливо при обычном предположении, что ширина полосы цепи мала по сравнению с обратной величиной периода синхросигнала.)

б) Если $s(t)$ — периодическая импульсная последовательность с периодом T и если $\max\limits_t s(t)=1$, то дисперсия ошибки времени равна

$$\sigma_\tau^2 = \frac{N_0 B_L}{A^2(2\pi\Delta f)^2}\,\frac{TS_2}{S_1^2},$$

где величина $S_i \underset{=}{\Delta} \int\limits_0^T (d^i s(t)/dt^i)^2 dt$ предполагается конечной как при $i=1$, так и при $i=2$.

6.6. Рассмотрим следующую схему определения фазы искаженной шумом псевдошумовой последовательности длины 2^k-1. В начале принимаются k последовательных битов, относительно них строится решение (с использованием методов гл. 4), и они заносятся в регистр сдвига, предназначенный для генерирования такой же последовательности, как и принятая. Затем строятся решения относительно последовательно принимаемых битов и сравниваются с соответствующим выходом регистра сдвига. Подсчитывается число случаев, когда выходы регистра сдвига и устройства, принимающего решение, совпадают, и на основе этого подсчета выполняется последовательный тест для того, чтобы определить, находятся ли в фазе местная и принимаемая последовательности. Если принимается решение о том, что они не в фазе, то новое множество из k битов, относительно которых приняты решения, вносится в регистр сдвига, и начинается новый последовательный тест. Эта процедура продолжается до тех пор, пока некоторый последовательный тест закончится принятием гипотезы о том, что две последовательности находятся в фазе. Оценить число принимаемых битов, необходимых для завершения синхропоиска, при вероятности ошибки, меньшей или равной P_e, и при выполнении следующих предположений:

а) синхронизация битов уже установлена;

б) если две последовательности не согласованы по фазе, то совпадение и несовпадение сравниваемых битов равновероятно: последовательные совпадения и несовпадения являются статистически независимыми событиями.

При каких отношениях сигнал/шум этот метод лучше методов, рассмотренных в § 6.7 и 6.8?

6.7. Показать, что псевдошумовая последовательность может быть отслежена системой ФАПЧ, использующей какой-либо из местных сигналов $z_1=p(t)-p(t-\Delta T)$ или

$$z_2(t)=\begin{cases} p(t), & l\,\Delta T < t < \left(l+\dfrac{1}{2}\right)\Delta T; \\ -p(t), & \left(l+\dfrac{1}{2}\right)\Delta T < t < (l+1)\,\Delta T, \quad l= \ldots -1, 0, 1, \ldots, \end{cases}$$

где $p(t)$ обозначает последовательность, а ΔT — ее период в битах. (Такое устройство называется *системой синхронизации с задержкой.*) Сравнить результирующие сигналы ошибок.

Глава 7

СИНХРОНИЗАЦИЯ СИМВОЛОВ ПО МАКСИМУМУ ПРАВДОПОДОБИЯ

7.1. Введение

Глава 6 была посвящена изучению методов установления отсчета времени и синхронизации более высокого порядка путем использования дополнительных каналов. В большинстве оставшихся глав так или иначе рассматриваются методы извлечения этой информации непосредственно из принимаемого сообщения. Основная цель состоит в том, чтобы полностью обойтись без всяких вспомогательных каналов синхронизации.

Очевидно, что информация, необходимая, в частности, для установления синхронизации символов, присутствует, фактически, в самом сигнале, переносящем сообщение. Очевидно, должно существовать ощутимое различие между принимаемыми символами для того, чтобы была передана какая-либо информация. А так как символы должны быть различимыми, можно, по-видимому, непосредственно по принимаемой последовательности определить, когда именно происходит переход (во времени) от одного символа к другому. Цель этой главы состоит в исследовании методов использования этой возможности.

7.2. Символьный синхронизатор максимального правдоподобия

В этом параграфе принцип максимума правдоподобия применяется к задаче синхронизации символов. Решение максимального правдоподобия относительно метки символа состоит в принятии такой метки[1] ν, которая максимизирует функцию $p[y(t)|\nu]$ и, следовательно, определяет метку символа, наиболее правдоподобно отвечающую наблюдаемому сигналу $y(t)$. Развивая этот подход, будем предполагать, что все символы имеют равную и известную длительность T_s секунд. Всякое устройство, которое пытается установить метку символа, будет называться *символьным синхронизатором*; синхронизатор, который находит максимум по ν плотностей вероятностей $p[y(t)|\nu]$, будет называться *символьным синхронизатором максимального правдоподобия*.

Вывод математического вида синхронизатора максимального правдоподобия аналогичен выводу для приемника максимального правдоподобия в гл. 3. Пусть принимаемый сигнал $y(t)=x_j(t-\nu\Delta T)+n(t)$ пропускается через идеальный фильтр нижних частот с шириной полосы B и производятся выборки со скоростью $2B$ выборок в секунду (см. § 3.4). Выходом является последовательность выборок

---

[1] Так же, как и в гл. 6, удобно ограничить рассмотрение вначале лишь случаем, в котором имеется только конечное число конкурирующих меток. *(Прим. авт.)*.

$$y_i = x^j_{i-\nu k} + n_i \begin{cases} j = 0,\ 1,\ \cdot\cdot\cdot, ML + (N-1)\,k; \\ j = 1,\ 2,\ \cdot\cdot\cdot, n. \end{cases} \tag{7.1}$$

Слагаемые n_i — это независимые выборки гауссовского случайного процесса, имеющего нулевое среднее и дисперсию $\sigma^2=N_0B$, где N_0, как обычно, обозначает одностороннюю спектральную плотность шума. Надстрочный индекс j обозначает j-й символ из множества n возможных символов $x_j(t)$; L — число выборок на символ; $k=L\Delta T/T_s$ — число выборок в интервале, разделяющем любые две последовательные метки символов; M обозначает полное число наблюдаемых символов. Наконец, метка ν является некоторым целым числом из интервала $\{0, N-1\}$.

Так как множество наблюдаемых $Y=\{y_i\}$ представляет собой множество независимых гауссовских величин, то, когда j и ν заданы, имеем

$$p(Y\,|\,\nu) = \prod_{l=0}^{M-1} \sum_{j=1}^{n} \frac{1}{(\sqrt{2\pi}\,\sigma)^L} \exp\left\{-\frac{1}{2\sigma^2} \sum_{i=lL+\nu k}^{(l+1)\,L+\nu k-1} (y_i - x^j_{i-\nu k})^2\right\} P(j) =$$

$$= K_1 \prod_{l=0}^{M-1} \sum_{j=1}^{n} \exp\left\{\frac{1}{\sigma^2} \sum_{i=lL+\nu k}^{(l+1)\,L+\nu k-1} y_i x^j_{i-\nu k} - \frac{1}{2}\,(x^j_{i-\nu k})^2\right\} P(j), \tag{7.2}$$

где $P(j)$ — вероятность j-го символа и

$$K_1 = \frac{1}{(\sqrt{2\pi}\sigma)^{ML}} \exp\left\{-\frac{1}{2\sigma^2} \sum_{i=\nu k}^{ML+\nu k-1} y_i^2\right\}.$$

Заметим, что крайние выборки y_i с номерами $0\leqslant i<\nu k$ и $ML+\nu k\leqslant i<(M+1)L$ в равенстве (7.2) опущены. Множество наблюдаемых Y обязательно содержит все выборки y_i, $0\leqslant i<(M+1)\,L$, так как выражения $p(Y|\nu)$ должны быть вычислены для всех ν. Пренебрежение этими крайними выборками приводит к потере некоторой информации, от которой может зависеть решение. Тем не менее, если число выборок $(M+1)L$, требуемых для надежного решения, велико, то эти крайние выборки вносят пренебрежимо малый вклад в общую имеющуюся в распоряжении информацию и могут быть без ущерба опущены. При очень больших отношениях сигнал/шум это неверно, как вскоре будет показано. Однако с этим исключением использование крайних выборок в нижеследующих выкладках лишь усложнит результаты, не изменив их существенно. С той же оговоркой множитель K_1 в ф-ле (7.2), по существу, не зависит от ν и, следовательно, может рассматриваться как константа.

Взяв предел в суммах (7.2) при стремлении ширины полосы B к бесконечности и стремлении к нулю интервала между выборками, находим, что решение максимального правдоподобия состоит в выборе той метки символа ν, для которой достигает максимума выражение

$$\prod_{l=0}^{M-1}\left(\sum_{j=1}^{n}\exp\left\{\frac{1}{N_0}\int\limits_{lT_s+\nu\Delta T}^{(l+1)T_s+\nu\Delta T}[2y(t)\,x_j(t-\nu\Delta T)-x_j^2(t-\nu\Delta T)]\,dt\right\}P(j)\right). \tag{7.3}$$

Это и есть та математическая операция, которую должен выполнить синхронизатор максимального правдоподобия.

Другой часто используемый подход состоит в том, что одновременно выносится решение максимального правдоподобия относительно метки и о символах $x_j(t-\nu\Delta T)$. В этом случае (7.3) следует, очевидно, заменить на

$$\prod_{l=0}^{M-1}\left[\max_{j_l}\exp\left\{\frac{1}{N_0}\int\limits_{lT_s+\nu\Delta T}^{(l+1)T_s+\nu\Delta T}[2y(t)\,x_{j_l}(t-\nu\Delta T)-x_{j_l}^2(t-\nu\Delta T)]\,dt\right\}\right]. \tag{7.4}$$

Так как некоторая информация неизбежно теряется при замене (7.3) на (7.4), получающийся синхронизатор будет в какой-то мере хуже синхронизатора максимального правдоподобия. Однако, как будет показано, ф-ла (7.4) часто приводит к намного более приемлемому для практики устройству. Более того, такой подход может быть подходящим, когда неизвестны априорные вероятности $P(j)$. [Еще одной возможностью является вынесение решения по максимуму апостериорной вероятности относительно символов и решения максимального правдоподобия относительно метки. Единственным отличием этого метода от только что рассмотренного является использование априорных вероятностей при отыскании максимума сомножителей по j в ф-ле (7.4).]

При получении (7.3) и (7.4) мы неявно предполагали, что точно известен вид функций $x_j(t-\tau)$, соответствующих символам, за исключением случайной временной задержки τ. Это предположение часто оказывается справедливым. Например, если имеется фазово-когерентный отсчет времени, то эта предполагаемая возможность воспроизведения символов (с точностью до их временно́й задержки) в приемнике может на самом деле существовать. Однако не так уж редко имеются и другие неизвестные параметры, даже тогда, когда делается попытка установить синхронизацию символов.

Параметром, который чаще всего не известен, является фаза несущей. В этом случае распределение множества наблюдаемых Y является функцией фазы несущей и метки ν. Если предполагается, что фаза несущей постоянна в течение каждого интервала передачи (это предположение согласуется с тем, которое было сделано при обсуждении некогерентного по фазе приема), то фазовонекогерентный символьный синхронизатор максимального правдоподобия должен вычислять выражение

$$\int \dots \int p(Y \mid \nu,\ \Phi_1\ \ \Phi_2,\ \dots \Phi_M)\, p(\Phi_1,\ \Phi_2,\ \dots,\Phi_M) \times$$
$$\times\, d\,\Phi_1\, d\,\Phi_2 \dots d\Phi_M, \tag{7.5}$$

где Φ_i — фаза в течение i-го интервала; $iT_s+\nu\Delta T<t<(i+1)T_s+$ $+\nu\Delta T$. Как и в § 6.6, вид синхронизатора зависит от предположений относительно плотности распределения $p(\Phi_1,\ \Phi_2,\ \dots,\ \Phi_M)$. Рассмотрение здесь будет ограничено синхронизаторами, которые получаются в приближении

$$p(\Phi_1,\ \Phi_2,\ \dots,\Phi_M) = p(\Phi_1)\, p(\Phi_2)\ \dots\ p(\Phi_M). \tag{7.6}$$

(Очевидно, можно предполагать, что статистики фазы также не зависят от метки символа ν.) Если существует некоторая зависимость фаз последовательных символов (а она неизбежно существует), то это приближение приводит к подоптимальному синхронизатору, в котором некоторая информация о фазе отбрасывается вместо того, чтобы быть использованной. Тем не менее характеристика этого подоптимального синхронизатора служит границей снизу для характеристики оптимального синхронизатора, в котором используется вся информация о фазе. Граница сверху для этой характеристики устанавливается, конечно, с помощью фазовокогерентного синхронизатора (ср. с § 6.6).

Используя равенство (7.6), находим, что максимально правдоподобной меткой символа будет ν, которое максимизирует выражение

$$\prod_{l=0}^{M-1} \left(\sum_{j=1}^{n} \int p(\Phi) \left\{ \exp \frac{1}{N_0} \int\limits_{lT_s+\nu\Delta T}^{(l+1)\,T_s+\nu\Delta T} [2y(t)\, x_j(t-\nu\Delta T,\ \Phi) - \right.\right.$$
$$\left.\left. - [x_j(t-\nu\Delta T,\Phi)]^2]\, dt \right\} d\,\Phi\, P(j) \right). \tag{7.7}$$

Вновь непосредственным видоизменением синхронизатора максимального правдоподобия является такой, который выносит совместные решения максимального правдоподобия относительно меток, символов и возможно даже фаз. Этот синхронизатор находит метку ν, которая максимизирует функцию

$$\prod_{l=0}^{M-1} \max_{j_l} \int p(\Phi) \left\{ \exp \frac{1}{N_0} \int\limits_{lT_s+\nu\Delta T}^{(l+1)\,T_s+\nu\Delta T} [2y(t)\, x_{j_l}(t-\nu\Delta T,\Phi) - \right.$$
$$\left. - [x_{j_l}(t-\nu\Delta T,\ \Phi)^2\,]\, dt \right\} d\,\Phi \tag{7.8}$$

или функцию

$$\prod_{l=0}^{M-1} \max_{j_l,\, \Phi_l} \exp \frac{1}{N_0} \int\limits_{lT_s+\nu\Delta T}^{(l+1)\,T_s+\nu\Delta T} [2y(t)\, x_{j_l}(t-\nu\Delta T,\ \Phi_l) - \\ - [x_{j_l}(t-\nu\Delta T,\ \Phi_l)]^2\,]\, dt. \qquad (7.9)$$

Кроме временно́й задержки и фазы несущей, могут быть неизвестными также другие параметры, например, амплитуда символа или спектральная плотность шума не всегда известны точно. В общем, однако, эти параметры можно достаточно точно оценить, чтобы обращаться с ними, как с известными, и при определении структуры требуемого синхронизатора связанные с ними неопределенности обычно можно игнорировать.

7.3. Синхронизация символов АИМ

Для описанных в § 3.5 и 3.6 систем амплитудно-импульсной модуляции рассмотрим фазовокогерентные и фазовонекогерентные символьные синхронизаторы максимального правдоподобия. Начнем с случая синхронизатора, для которого фаза несущей уже была определена.

Принимаемый сигнал имеет вид $y(t)=\sqrt{2}Ax\sin(\omega_c t+\Phi)+ +n(t)$, где A и Φ — известные постоянные, а x — случайная величина, постоянная на каждом интервале $iT_s+\nu\Delta T<t<(i+1)T_s+\nu\Delta T$ и имеющая известную априорную плотность распределения вероятности $p(x)$. Сумма по j в ф-ле (7.3) становится здесь интегралом, а вероятность $P(j)$ — плотностью вероятности. Максимально правдоподобной меткой ν является та, которая максимизирует

$$\prod_{l} \int\limits_{-\infty}^{\infty} \exp \left\{ \frac{1}{N_0} \int\limits_{lT_s+\nu\Delta T}^{(l+1)\,T_s+\nu\Delta T} [2Axy(t)\sqrt{2}\sin(\omega_c t+\Phi) - A^2x^2]\, dt \right\} p(x)\, dx. \qquad (7.10)$$

Это произведение может быть записано в виде

$$\prod_{l} e^{Ra_{\nu l}^2} \int\limits_{-\infty}^{\infty} e^{-R\,(x-a_{\nu l})^2}\, p(x)\, dx, \qquad (7.11)$$

где $R=A^2T_s/N_0$ и

$$a_{\nu l} \overset{\Delta}{=} \frac{1}{AT_s} \int\limits_{lT_s+\nu\Delta T}^{(l+1)\,T_s+\nu\Delta T} y(t)\sqrt{2}\sin(\omega_c t+\Phi)\, dt.$$

Интеграл

$$\frac{R^{1/2}}{\sqrt{\pi}} \int\limits_{-\infty}^{\infty} e^{-R\,(x-a_{\nu l})^2}\, p(x)\, dx \qquad (7.12)$$

является сверткой плотности распределения $p(x)$ и

$$p(a_{\nu l}) = \frac{R^{1/2}}{\sqrt{\pi}} e^{-Ra_{\nu l}^2}. \qquad (7.13)$$

Это соотношение отражает тот факт, что экспоненциальному члену $\exp(Ra_{\nu l}^2)$ нужно дать меньший вес, когда $a_{\nu l}$ существенно отличается от тех значений, которые предсказываются априорным распределением ее ожидаемой величины x. В общем, однако, этот член не влияет сильно на решение, принятое синхронизатором.

Для того чтобы обосновать это утверждение, когда x имеет равномерное распределение, рассмотрим интеграл из ф-лы (7.12) в двух крайних случаях, когда $R \gg 1$ и когда $R \ll 1$. Если $R \gg 1$, экспонента $e^{-R(x-a_{\nu l})^2}$ пренебрежимо мала, за исключением случая, когда $x \approx a_{\nu l}$. Если $p(x) = 1/(x_0 - x_1)$ для $x_1 < x < x_0$, то имеем

$$\frac{R^{1/2}}{\sqrt{\pi}} \int_{x_1}^{x_0} e^{-R(x-a_{\nu l})^2} p(x)\,dx \approx \begin{cases} \dfrac{1}{x_0 - x_1} & \text{при } x_1 < a_{\nu l} < x_0; \\ 0 & \text{в остальных случаях.} \end{cases}$$

Но когда R велико, $a_{\nu l}$ будут с большой вероятностью оставаться внутри интервала (x_1, x_0), так что взвешивающая функция почти везде постоянна.

Аналогично, если $R \ll 1$, то $e^{-R(x-a_{\nu l})^2} \approx 1$, кроме случая, когда $a_{\nu l}$ значительно выходят из интервала (x_1, x_0). В этом случае

$$\frac{R^{1/2}}{\sqrt{\pi}} \int_{x_1}^{x_0} e^{-R(x-a_{\nu l})^2} p(x)\,dx \approx \frac{R^{1/2}}{\sqrt{\pi}},$$

и это выражение вновь, по существу, постоянно.

Когда x имеет гауссовское распределение $p(x) = (1/\sqrt{2\pi}\sigma_s) e^{-x^2/2\sigma_s^2}$, ситуация становится даже более простой. При этом

$$\frac{R^{1/2}}{\sqrt{\pi}} \int_{-\infty}^{\infty} e^{-R(x-a_{\nu l})^2} p(x)\,dx = \frac{1}{\sqrt{\pi}} \left(\frac{1}{1+2R\sigma_s^2}\right)^{1/2} \times e^{-[R/(1+2R\sigma_s^2)]\,a_{\nu l}^2}$$

и (7.11) принимает вид

$$K \prod_l e^{[(2R\sigma_s^2)/(1+2R\sigma_s^2)]\,a_{\nu l}^2}.$$

Но так как ν, максимизирующее выражение $K_1 \prod_l \exp(K_2 a_{\nu l}^2)$, не зависит от K_1 и K_2, то решение остается одним и тем же независимо от того, включается ли множитель в интеграл (7.12) или нет.

В качестве последнего аргумента в пользу приравнивания выражения (7.12) постоянной, заметим, что когда производится совместное решение максимального правдоподобия относительно символа и метки [см. (7.4)], это выражение заменяется на постоянную

$$\max_x \left[\frac{R^{1/2}}{\sqrt{\pi}} e^{-R\left(x-a_{\nu l}\right)^2} \right] = \frac{R^{1/2}}{\sqrt{\pi}} . \tag{7.14}$$

С этими оговорками будем пренебрегать интегралом в (7.11), считая его постоянной и понимая, что получающийся синхронизатор, возможно, будет подоптимальным. Относительная простота статистики

$$z'_\nu = \prod_l e^{Ra_{\nu l}^2} \tag{7.15}$$

обычно вполне компенсирует эту возможную подоптимальность. Как обычно, более удобно работать с логарифмом статистики, а не с самой статистикой. Определим с этой целью

$$z_\nu = \sum_l a_{\nu l}^2 . \tag{7.16}$$

Если число слагаемых в каждой из этих сумм велико, то можно использовать центральную предельную теорему для того, чтобы показать, что z_ν имеет приближенно гауссовское распределение 1). Вероятность того, что правильная метка символа (которая без потери общности будет предполагаться нулевой меткой $\nu=0$) может быть правильно опознана среди всех других меток, также можно выразить с помощью первых и вторых моментов случайных величин z_ν .

Пусть M обозначает полное число слагаемых в сумме (7.16) и пусть $m=E(x)$ — математическое ожидание амплитуды сигнала; $\mu_i=E[(x-m)^i]$ — ее i-й центральный момент и $R=A^2T_s/N_0$ — отношение сигнал/шум на входе (см. § 3.5). Пусть далее $\lambda_\nu=\nu\Delta T/T_s=$ $=\nu/N$. Первые и вторые моменты случайных величин z_ν могут быть выражены с помощью этих параметров следующим образом:

$$\eta_\nu = E(z_\nu) = M\left\{\left[(1-\lambda_\nu)^2+\lambda_\nu^2\right]\mu_2 + m^2 + \frac{1}{2R}\right\} ; \tag{7.17}$$

$$\sigma_\nu^2 = M\sigma_{sxs}^2 + M\sigma_{sxn}^2 + M\sigma_{nxn}^2 , \tag{7.18}$$

где $\sigma_{sxs}^2 = \left[\lambda_\nu^2 + (1-\lambda_\nu)^2\right]^2 (\mu_4-\mu_2^2) + 4\left[\lambda_\nu^2 + (1-\lambda_\nu)^2\right] m\mu_3 +$ $+ 4\lambda_\nu^2(1-\lambda_\nu)^2\mu_2^2 + 4m^2\mu_2$; $\sigma_{sxn}^2 = \left\{\left[(1-\lambda_\nu)^2+\lambda_\nu^2\right]\mu_2 + m^2\right\} \dfrac{2}{R}$ и $\sigma_{nxn}^2 = 1/2R^2$.

---

1) Опять-таки легко устанавливаемое существование вторых моментов одинаково распределенных случайных величин $a_{\nu l}^2$ оправдывает это утверждение. Величины $a_{\nu l}^2$ и $a_{\nu,\, l+i}^2$ статистически независимы для всех $i\neq 0,1$. Следовательно, суммы $\sum\limits_{\text{по нечетным } l} a_{\nu l}^2$ и $\sum\limits_{\text{по четным } l} a_{\nu l}^2$ асимптотически имеют гауссовское распределение, и так как z_ν является суммой двух гауссовских случайных величин, то z_ν также гауссовская величина. (*Прим. авт.*).

Подстрочные индексы в последних трех членах обозначают соответственно «сигнал/сигнал» (дисперсия, обусловленная лишь сигналом), «сигнал/шум» (дисперсия, обусловленная взаимодействием сигнала и шума) и «шум/шум» (дисперсия, обязанная лишь шуму) [1].

Окончательно

$$\Delta^2_{\nu\mu} \underline{\underline{\Delta}} E\left[\left(z_\nu - z_\mu\right)^2\right] - E^2\left(z_\nu - z_\mu\right) = M\Delta^2_{sxs} + M\Delta^2_{sxn} + M\Delta^2_{nxn}, \quad (7.19)$$

где $\Delta^2_{sxs} = 4(\lambda_\mu - \lambda_\nu)^2\left[1 - (\lambda_\mu + \lambda_\nu)\right]^2 \mu_4$; $\Delta^2_{sxn} = 4(\lambda_\mu - \lambda_\nu)\left[1 - (2\lambda_\nu + \lambda_\mu) + 3\lambda_\nu\lambda_\mu\right]\frac{\mu_2}{R}$; $\Delta^2_{nxn} = 2(\lambda_\mu - \lambda_\nu)\left[1 - (\lambda_\mu - \lambda_\nu)\right]\frac{1}{R^2}$

и $\mu \geqslant \nu$. Вновь подчеркнем, что эти выражения были получены в предположении, что M — число наблюдаемых символов — достаточно велико для того, чтобы при рассмотрении опустить часть символов в начале и в конце интервала наблюдения.

Если все метки проверяются одновременно, то вероятность ошибочного решения, как обычно, оценивается следующим образом:

$$\max_{i \neq 0} \Pr\{z_0 - z_i < 0\} \leqslant P_e = 1 - \Pr\left\{z_0 > \max_{i \neq 0} z_i\right\} \leqslant \sum_{i=1}^{N-1} \Pr\{z_0 - z_i < 0\} \leqslant$$

$$\leqslant (N-1)\max_{i \neq 0} \Pr\{z_0 - z_i < 0\}. \quad (7.20)$$

Когда M достаточно велико, чтобы оправдать использование гауссовской аппроксимации для распределения случайных величин z_i, случайная величина $y_i = z_0 - z_i$ также имеет гауссовское распределение со средним значением

$$m_i = E(y_i) = \eta_0 - \eta_i \quad (7.21)$$

и дисперсией

$$\sigma_i^2 = E(y_i^2) - E^2(y_i) = \Delta^2_{0i}, \quad (7.22)$$

которые определяются равенствами (7.17)—(7.19) соответственно. Производя решения так же, как в § 6.4, но параллельно, получаем, что если вероятность ошибки мала, то наименьшее из отношений

$$\frac{m_i^2}{\sigma_i^2} = \frac{2M\lambda_i(1 - \lambda_i)\mu_2^2}{2\lambda_i(1 - \lambda_i)\mu_4 + 2\mu_2/R + 1/R^2} \quad (7.23)$$

должно быть порядка $2K_N \log_e 1/P_e$. (Коэффициент K_N, напомним, ограничен снизу единицей и сверху величиной $1+$

---

[1] Во всех этих выражениях ω_c предполагается либо равной некоторому целому кратному величины $2\pi/\Delta T$, либо достаточно большой по сравнению с шириной полосы сигнала, так что несущая может быть устранена демодулятором, который формирует произведение (ср. с § 3.4). Это предположение нужно лишь для упрощения получающихся результатов; оно существенно не изменяет условия. Если несущая не удовлетворяет ни одному из этих предположений, то время синхронизации, по-видимому, уменьшится в силу того, что некоторые из конкурирующих меток будут более явно отличаться от правильной метки. (*Прим. авт.*).

$+\log_e(N-1)/\log_e(1/P_e)$; если, как в обычно рассматриваемых случаях, $P_e \ll 1/N$, то K_N, по существу, равен единице.) Это отношение является возрастающей функцией λ_i при $\lambda_i<1/2$ и убывающей функцией λ_i при $\lambda_i>1/2$. Таким образом, оно достигает минимума при $\lambda_i=1/N$ (и $\lambda_i=1-1/N$). Полное число символов M_T, необходимых для решения, следовательно, равно

$$M_T = 2NK_N \log_e \frac{1}{P_e}\left[\frac{\mu_4}{N\mu_2^2} + \frac{N}{N-1}\left(\frac{1}{R\,\mu_2} + \frac{1}{2R^2\,\mu_2^2}\right)\right]. \tag{7.24}$$

Интересно сравнить этот результат с аналогичным результатом гл. 6. Зависимость времени поиска от N в обоих случаях является одной и той же, если ширина автокорреляционной функции синхросигнала порядка $T_s/2$. Наличие выражений $1/R$ и $1/R^2$ в (7.24) напоминает случай фазовонекогерентного приема, рассмотренный в гл. 6. Это не удивительно, так как в обоих случаях при принятии решения используется квадрат интеграла от сигнала, сложенного с гауссовским шумом.

Когда R стремится к бесконечности, отношение (7.23) стремится к $M\mu_2^2/\mu_4$, а это означает, что ошибки синхронизации возможны даже в отсутствие шума. Это происходит потому, что краевые эффекты становятся все более и более существенными при $R\to\infty$. Тем не менее правильное решение может всегда быть принято на основе статистики z_ν [равенство (7.16)] даже после наблюдения лишь одного символьного интервала в случае, когда шума нет. Чтобы доказать это, необходимо лишь учесть, что выражение

$$\int\limits_{\tau_1}^{\tau_2} y^2(t)\,dt - \frac{\left[\int\limits_{\tau_1}^{\tau_2} \sqrt{2}\,y(t)\sin\omega_c(t-\tau)\,dt\right]^2}{\int\limits_{\tau_1}^{\tau} 2\sin^2\omega_c(t-\tau)\,dt} - \frac{\left[\int\limits_{\tau}^{\tau_2} \sqrt{2}\,y(t)\sin\omega_c(t-\tau)\,dt\right]^2}{\int\limits_{\tau}^{\tau_2} 2\sin^2\omega_c(t-\tau)\,dt}, \quad \tau_1<\tau<\tau_2$$

положительно, кроме случая, когда сигнал $y(t)$ представляет собой синусоиду с постоянной амплитудой в каждом из двух интервалов интегрирования, т. е. кроме случая, когда $y(t)=x_1\sin\omega_c(t-\tau)$, $\tau_1<t<\tau$ и $y(t)=x_2\sin\omega_c(t-\tau)$, $\tau<t<\tau_2$ [1]. Таким образом, сумма двух последних членов достигает максимума, когда $\tau=\nu\Delta T$, где ν — правильная метка символа. Этот максимум будет единственным, кроме случая, когда $y(t)$ постоянна на всем интервале $\tau_1<$

---

[1] Это утверждение является прямым следствием неравенства Шварца. *(Прим. авт.).*

$<t<\tau_2$, что может случиться только, если два последовательных символа равны (событие, которое имеет нулевую вероятность при рассматриваемых здесь условиях) или если область интегрирования полностью содержится в односимвольном интервале. Соответственно абсолютно надежное решение может быть сделано на основе этих двух последних членов (в отсутствие шума) лишь тогда, когда интервал наблюдения по меньшей мере равен T_s секунд. Однако только числители этих членов зависят от принимаемого сигнала, и эти числители фактически являются статистиками вида (7.16).

Если различные метки не могут быть проверены одновременно, можно использовать те же самые решающие переменные z_ν вместе с каким-либо из поочередных тестов, рассмотренных в гл. 6. Анализ этих различных синхронизационных схем с поочередной обработкой аналогичен во всех существенных деталях соответствующему анализу из гл. 6 и приводит к аналогичным результатам.

Синхронизатор максимального правдоподобия для фазовонекогерентной АИМ согласно ф-ле (7.7) определяет метку ν, которая максимизирует

$$\prod_l \frac{1}{2\pi}\int_0^{2\pi}\int_{-\infty}^{\infty}\exp\left\{\frac{1}{N_0}\int_{lT_s+\nu\Delta T}^{(l+1)T_s+\nu\Delta T}\left[2Axy(t)\sqrt{2}\sin(\omega_c t+\Phi)-A^2x^2\right]dt\right\}p(x)\,dx\,d\Phi. \tag{7.25}$$

(Для некогерентной АИМ мы приняли наши обычные предположения: принимаемый сигнал имеет вид $\sqrt{2}Ax\sin(\omega_c t+\Phi)$, где x имеет априорное распределение $p(x)$ и Φ равномерно распределена на интервале $(0,2\pi)$. Кроме того, $\omega_c=2\pi k/T_s$, где k — либо целое число, либо достаточно велико по сравнению с единицей.) Если определить

$$a_{\nu l}=\frac{1}{AT_s}\int_{lT_s+\nu\Delta T}^{(l+1)T_s+\nu\Delta T}\sqrt{2}\,y(t)\sin\omega_c t\,dt \tag{7.26}$$

и

$$b_{\nu l}=\frac{1}{AT_s}\int_{lT_s+\nu\Delta T}^{(l+1)T_s+\nu\Delta T}\sqrt{2}\,y(t)\cos\omega_c t\,dt$$

и поступить так же, как в случае фазовокогерентного приема, то (7.25) можно привести к виду

$$\prod_l \frac{1}{2\pi}\int_0^{2\pi}\exp\left[Rc_{\nu l}^2(\Phi)\right]\int_{-\infty}^{\infty}\exp\left[-R\left[x-c_{\nu l}(\Phi)\right]^2\right]p(x)\,dx\,d\Phi, \tag{7.27}$$

где $c_{\nu l}(\Phi)=a_{\nu l}\cos\Phi+b_{\nu l}\sin\Phi$ и R определено так же, как и ранее. Вновь, либо считая интеграл по x практически постоянным, либо вынося совместные решения максимального правдоподобия относительно метки и символов [см. ф-лу (7.8)], получим выражение, по которому будет определяться метка:

$$K\prod_{l}\frac{1}{2\pi}\int\limits_{0}^{2\pi}\exp\left[\frac{R}{2}\zeta_{\nu l}^{2}\left(1+\cos 2(\theta-\Phi)\right)\right]d\Phi, \tag{7.28}$$

где $a_{\nu l}=\zeta_{\nu l}\cos\theta$; $b_{\nu l}=\zeta_{\nu l}\sin\theta$ и K (по крайней мере, приближенно) — постоянная величина. Выполняя интегрирование и пренебрегая постоянными членами, получим

$$\prod_{l}\exp\left(\frac{R}{2}\zeta_{\nu l}^{2}\right)I_{0}\left(\frac{R}{2}\zeta_{\nu l}^{2}\right). \tag{7.29}$$

Как $\exp[(R/2)\zeta_{\nu l}^{2}]$, так и $I_0[(R/2)\zeta_{\nu l}^{2}]$ являются монотонными функциями $\zeta_{\nu l}^{2}$, а это значит, что $\zeta_{\nu l}^{2}$ сама может быть использована как удовлетворительная решающая переменная. Фактически, если $R\ll 1$, то

$$e^{(R/2)\,\zeta_{\nu l}^{2}}I_{0}\left(\frac{R}{2}\zeta_{\nu l}^{2}\right)\sim e^{(R/2)\,\zeta_{\nu l}^{2}}\left(1+\frac{1}{4}\left(\frac{R}{2}\right)^{2}\zeta_{\nu l}^{4}+\ldots\right)\sim e^{(R/2)\,\zeta_{\nu l}^{2}}. \tag{7.30}$$

А если $R\gg 1$, то

$$e^{(R/2)\,\zeta_{\nu l}^{2}}I_{0}\left(\frac{R}{2}\zeta_{\nu l}^{2}\right)\sim e^{R\zeta_{\nu l}^{2}}\left(1+\frac{1}{\frac{R}{2}\zeta_{\nu l}^{2}}+\ldots\right)\sim e^{R\zeta_{\nu l}^{2}}. \tag{7.31}$$

Это выражение также получается, если решение максимального правдоподобия принимается относительно всех неизвестных параметров: всех величин x и Φ, а также ν [см. (7.9)]. Взяв логарифм какого-нибудь из выражений (7.30) или (7.31), получаем для решающей переменной относительно метки выражение

$$z_{\nu}=\sum_{l}\zeta_{\nu l}^{2}=\sum_{l}\left(a_{\nu l}^{2}+b_{\nu l}^{2}\right). \tag{7.32}$$

Хотя эта решающая переменная, вообще говоря, подоптимальна, если известны априорные распределения x и Φ или одно из этих распределений, относительная простота, с которой она может быть вычислена в реальной системе связи, легко оправдывает ее применение. Более того, из предыдущих рассуждений следует, что получающийся в результате синхронизатор, по-видимому, будет работать столь же хорошо, как и синхронизаторы, для которых известны эти распределения.

Анализ характеристик полученного синхронизатора аналогичен анализу для фазовокогерентного синхронизатора. Единственное отличие состоит в том, что шумовой член в выражении для среднего значения и член «шум/шум» в выражении для дисперсии в равенствах (7.17)—(7.19) удваиваются по отношению к соответствующим выражениям для случая фазовокогерентного приема. Для дальнейших ссылок перепишем здесь эти выражения:

$$\left.\begin{aligned}
&\eta_\nu = E(z_\nu) = M\left\{[(1-\lambda_\nu)^2 + \lambda_\nu^2]\mu_2 + m^2 + \frac{c_0}{2R}\right\};\\
&\sigma_\nu^2 = M(\sigma_{sxs}^2 + \sigma_{sxn}^2 + \sigma_{nxn}^2);\\
&\sigma_{sxs}^2 = [(1-\lambda_\nu)^2 + \lambda_\nu^2]^2(\mu_4 - \mu_2^2) + 4[\lambda_\nu^2 +\\
&+ (1-\lambda_\nu)^2]\, m\,\mu_3 + 4\lambda_\nu^2(1-\lambda_\nu)^2\mu_2^2/c_1 + 4m^2\mu_2;\\
&\sigma_{sxn}^2 = \{[(1-\lambda_\nu)^2 + \lambda_\nu^2]\mu_2 + m^2\}\frac{2}{R};\\
&\sigma_{nxn}^2 = c_0/2R^2;\\
&\Delta_{\nu\mu}^2 = E(z_\nu - z_\mu)^2] - E^2(z_\nu - z_\mu) = M[\Delta_{sxs}^2 + \Delta_{sxn}^2 + \Delta_{nxn}^2];\\
&\Delta_{sxs}^2 = 4(\lambda_\mu - \lambda_\nu)^2[1 - (\lambda_\mu + \lambda_\nu)]^2\mu_4/c_1;\\
&\Delta_{sxn}^2 = 4(\lambda_\mu - \lambda_\nu)[1 - (2\lambda_\nu + \lambda_\mu) + 3\lambda_\mu\lambda_\nu]\frac{\mu_2}{R};\\
&\Delta_{nxn}^2 = 2c_0(\lambda_\mu - \lambda_\nu)[1 - (\lambda_\mu - \lambda_\nu)]\frac{1}{R^2},
\end{aligned}\right\}\qquad (7.33)$$

где $\mu \geqslant \nu$. Коэффициент c_0 равен 1 в случае когерентного и 2 в случае некогерентного приема; c_1 равен 1 в обоих случаях. Вскоре мы поясним причину, по которой был введен этот последний коэффициент.

7.4. Символьная синхронизация для ФТ

Рассматриваемая здесь система обсуждалась в § 4.5 и 3.7; в этой системе с равными вероятностями на любом заданном интервале символа T_s секунд передается один из n сигналов $x_i(t) = \sqrt{2}A\sin(\omega_c t + \Phi + \theta_i)$, где фаза Φ известна, а $\theta_i = 2\pi i/n$, $i = 1, 2, \ldots, n$. Из ф-лы (7.3) следует, что наиболее правдоподобная метка символа соответствует значению ν, которое максимизирует выражение

$$\prod_l \frac{1}{n}\sum_{j=1}^{n}\exp\left\{\frac{2A}{N_0}\int\limits_{lT_s+\nu\Delta T}^{(l+1)T_s+\nu\Delta T} y(t)\sqrt{2}\sin(\omega_c t + \Phi + \theta_j)\,dt\right\} =$$

$$= \prod_l \frac{1}{n}\sum_{j=1}^{n}\exp\{2R(a_{\nu l}\cos\theta_j + b_{\nu l}\sin\theta_j\},\qquad (7.34)$$

где

$$a_{\nu l}=\frac{1}{AT_s}\int\limits_{lT_S+\nu\Delta T}^{(l+1)\,T_S+\nu\Delta T} y(t)\sqrt{2}\sin(\omega_c t+\Phi)\,dt;$$

$$b_{\nu l}=\frac{1}{AT_s}\int\limits_{lT_S+\nu\Delta T}^{(1+l)\,T_S+\nu\Delta T} y(t)\sqrt{2}\cos(\omega_c t+\Phi)\,dt$$

и $R=A^2T_s/N_0$.

Опять-таки из-за трудностей реализации описываемого равенством (7.34) синхронизатора (не говоря уже о трудностях анализа его характеристики) представляет интерес получить какие-либо приближения к этому идеальному случаю. Вначале рассмотрим приближение при малом отношении сигнал/шум. Разложение экспоненциального члена в ф-ле (7.34) в ряд дает

$$\prod_l \frac{1}{n}\sum_{j=1}^{n}\exp\{2R\,(a_{\nu l}\cos\theta_j+b_{\nu l}\sin\theta_j)\}=\prod_l \frac{1}{n}\sum_{j=1}^{n}[1+2Ra_{\nu l}\times$$
$$\times\cos\theta_j+2Rb_{\nu l}\sin\theta_j+2R^2a_{\nu l}^2\cos^2\theta_j+4R^2a_{\nu l}\,b_{\nu l}\sin\theta_j\cos\theta_j+$$
$$+2R^2b_{\nu l}^2\sin^2\theta_j+O(R^3)]. \tag{7.35}$$

Так как $\theta_j=2\,\pi_j/n$, $j=1, 2, \ldots, n$, то $\sum\limits_{j=1}^{n}\cos k\,\theta_j=\sum\limits_{j=1}^{n}\sin k\,\theta_j=0$ для любого целого k, не кратного числу n. Равенство (7.35) поэтому принимает вид

$$\prod_l\left[1+\frac{1+\delta_{n2}}{2}\,2R^2a_{\nu l}^2+\frac{1-\delta_{n2}}{2}\,2R^2b_{\nu l}^2+O(R^3)\right]\approx$$
$$\approx\begin{cases} K_1\sum\limits_l(a_{\nu l}^2+b_{\nu l}^2), & n>2;\\ K_2\sum\limits_l a_{\nu l}^2, & n=2,\end{cases} \tag{7.36}$$

где $\delta_{n2}=1$, когда $n=2$, и равно нулю в остальных случаях и где K_1 и K_2 не зависят от ν. Это приближение справедливо также для непрерывной ФТ; суммирование по j становится в этом случае интегрированием по θ.

Анализ характеристики приближения (7.36) к синхронизатору максимального правдоподобия полностью аналогичен приведенному выше анализу для случая АИМ. Действительно, если $n=2$ $(z_\nu=\sum\limits_l a_{\nu l}^2)$, первые два момента величины z_ν совпадают с аналогичными моментами для решающей переменной в случае фазовокогерентной АИМ [равенство (7.33) при $m=0$, $\mu_2=\mu_4=c_0=c_1=1$].

Если $n>2$ $(z_\nu = \sum_l a_{\nu l}^2 + b_{\nu l}^2)$, первые два момента величины z_ν также задаются ф-лами (7.33), но теперь $m=0$, $\mu_2=\mu_4=1$ и $c_0=c_1=2$ 1). Таким образом (при параллельном наблюдении), надежное решение относительно правильной метки получается, если число наблюдаемых символов порядка

$$M_T \approx 2N\kappa_N \log_e \frac{1}{P_e}\left(\frac{1}{N}+\frac{1}{R}+\frac{1}{2R^2}\right), \tag{7.37}$$

если $n=2$, и порядка

$$M_T \approx 2N\kappa_N \log_e \frac{1}{P_e}\left(\frac{1}{2N}+\frac{1}{R}+\frac{1}{2R^2}\right), \tag{7.38}$$

если $n>2$ [ср. с равенством (7.24)].

Интересно отметить, что оптимальный синхронизатор для когерентных сигналов ОФТ при малом отношении сигнал/шум эквивалентен (кроме случая, когда $n=2$) синхронизатору, полученному для случая когерентного приема. В отсутствие опорной фазы выражение (7.34) заменяется на

$$\prod_l \frac{1}{n}\sum_{j=1}^{n}\frac{1}{2\pi}\int_0^{2\pi}\exp\left\{2R\left(a_{\nu l}\cos(\theta_j+\Phi)+b_{\nu l}\sin(\theta_j+\Phi)\right)\right\}d\Phi =$$

$$=\prod_l I_0\left(2R\left(a_{\nu l}^2+b_{\nu l}^2\right)^{1/2}\right), \tag{7.39}$$

где $a_{\nu l}$ и $b_{\nu l}$ были определены ранее [см. (7.34)], но теперь имеют произвольную местную фазу Φ. Используя разложение функции Бесселя для малых значений аргумента, так же как в § 7.3, получим приближение к (7.39) для малого отношения сигнал/шум в виде

$$\prod_l \left[1+R^2\left(a_{\nu l}^2+b_{\nu l}^2\right)+O(R^4)\right]; \tag{7.40}$$

это означает, что решение относительно правильной метки символа должно основываться на выражениях

$$z_\nu = \sum_l \left(a_{\nu l}^2+b_{\nu l}^2\right) \tag{7.41}$$

независимо от значения n. Исключая случай, когда $n=2$, этот вывод совпадает с утверждением, полученным в случае когерентного приема, а соответствующие синхронизаторы имеют одинаковые характеристики. Характеристика двоичного относительного когерентного синхронизатора, очевидно, эквивалентна характеристике двоичного синхронизатора для фазовонекогерентной АИМ, рассмотренной в предыдущем параграфе, если положить $m=0$ и $\mu_2=\mu_4=1$.

---

1) Здесь последовательные фазы предполагаются статистически независимыми и равномерно распределенными. Для видоизменения этих результатов в случае, когда это последнее ограничение снимается, см. задачу 7.1. (*Прим. авт.*).

Действительно, не должно удивлять то, что синхронизаторы для фазовокогерентной и относительной когерентной ФМ совпадают. Как в той, так и в другой ситуации информация о метке символа содержится в изменениях фазы при переходе от одного символа к другому; характеристика синхронизатора зависит от разности фаз, а не от самого значения фазы.

В другом предельном случае, когда отношение сигнал/шум R велико по сравнению с единицей, слагаемое в сумме (7.34), для которого величина $(a_{\nu l}\cos\theta_j+b_{\nu l}\sin\theta_j)$ максимальна, по-видимому, будет много больше, чем остальная часть этой суммы. При этом предположении логарифм выражения (7.34) будет пропорционален

$$\sum_l \max_{j_l}\{a_{\nu l}\cos\theta_{j_l}+b_{\nu l}\sin\theta_{j_l}\}. \tag{7.42}$$

Это выражение получилось бы, если бы мы попытались получить совместное решение относительно метки и символов [см. (7.4)]. Значение θ_j, максимизирующее выражение $a_{\nu l}\cos\theta_j+b_{\nu l}\sin\theta_j$, равно θ_k, где $|\theta-\theta_k|\leqslant\frac{\pi}{n}$; $\theta=\operatorname{arctg}(b_{\nu l}/a_{\nu l})$ (см. § 4.5). Если n велико, то $\theta\approx\theta_k$ для некоторого k и

$$\max_j\{a_{\nu l}\cos\theta_j+b_{\nu l}\sin\theta_j\}=(a_{\nu l}^2+b_{\nu l}^2)^{1/2}\cos(\theta-\theta_k)\approx(a_{\nu l}^2+b_{\nu l}^2)^{1/2}. \tag{7.43}$$

В противоположность этому, если $n=2$ (с $\theta_j=0$ или π), то

$$\max_j\{a_{\nu l}\cos\theta_j+b_{\nu l}\sin\theta_j\}=|a_{\nu l}|. \tag{7.44}$$

Относительный когерентный синхронизатор (7.39) можно аппроксимировать, когда R велико, используя асимптотическое разложение функции Бесселя

$$\prod_l I_0[2R(a_{\nu l}^2+b_{\nu l}^2)^{1/2}]\sim\prod_l\exp\{2R(a_{\nu l}^2+b_{\nu l}^2)^{1/2}\}. \tag{7.45}$$

То же выражение получается, когда производится совместная оценка максимального правдоподобия для фазы Φ и символа j:

$$\prod_l \max_{j_l\,\Phi_l}\exp\{2R[a_{\nu l}\cos(\theta_{j_l}+\Phi_l)+b_{\nu l}\sin(\theta_{j_l}+\Phi_l)]\}=$$

$$=\prod_l\exp\{2R(a_{\nu l}^2+b_{\nu l}^2)^{1/2}\}. \tag{7.46}$$

В каждом из этих случаев решение должно основываться на переменных

$$z'_\nu=\sum(a_{\nu l}^2+b_{\nu l}^2)^{1/2}. \tag{7.47}$$

Наилучшее приближение к синхронизатору максимального правдоподобия зависит, очевидно, как от отношения сигнал/шум, так и от числа возможных фаз. Однако, как и в § 6.6, можно достаточно обоснованно ограничиться лишь приближениями для малых отношений сигнал/шум. Это, в конце концов, представляет наиболее трудную для синхронизации ситуацию. Более того, характеристика такого синхронизатора дает нижнюю границу для характеристики идеального синхронизатора. Наконец (и это, возможно, самое важное) для этих приближений к идеальному синхронизатору характеристика, относящаяся к большим отношениям сигнал/шум (если интересуются лишь эффектами, связанными с шумом), фактически совпадает с характеристикой оптимального синхронизатора в отсутствие какой-либо модуляции. Запас для возможного улучшения характеристики здесь очень небольшой. Чтобы показать это, нужно лишь сравнить ф-лы (7.37), (7.38), (7.24) с (6.19) и заметить, что в рассматриваемом случае $\max_i \rho(iT_s/N) = 1 - 1/N$.

7.5. Синхронизация ортогональных символов

В нескольких предыдущих параграфах подход к задаче синхронизации символов, описанный во введении к этой главе, был применен к АИМ и ФТ системам связи. Тот же самый подход в равной мере применим к ортогональным (и биортогональным) системам связи, рассмотренным в гл. 4. Практическая значимость этого подхода зависит от того, какое конкретное множество ортогональных символов используется. В последующих главах будут описаны конструкции ортогональных символов, которые значительно лучше приспособлены к методам эффективной синхронизации, чем любая из двух конструкций (ВИМ и ЧТ), рассмотренных в гл. 4. Поэтому обсуждение задачи синхронизации в применении к этим двум классам множеств символов будет кратким.

Синхронизация ЧТ символов. Если множество символов имеет вид

$$x_i(t) = \sqrt{2}\sin\omega_i t, \quad 0 < t < T_s, \quad i = 1, 2, \ldots, n, \qquad (7.48)$$

где $\omega_i = \pi k_i/T_s$; k_i — некоторое целое (ср. с § 4.4), то статистики фазовокогерентного синхронизатора максимального правдоподобия [см. (7.3)] принимают вид

$$\prod_l \sum_{j=1}^{n} \exp[2Rz_{\nu l}(j)]\,P(j), \qquad (7.49)$$

где

$$z_{\nu l}(j) = \frac{1}{AT_s} \int\limits_{lT_s+\nu\Delta T}^{(l+1)T_s+\nu\Delta T} \sqrt{2}\,y(t)\sin\omega_j(t - lT_s - \nu\Delta T)\,dt$$

и $R = A^2T_s/N_0$. Здесь опять были опущены члены, которые не зависят от ν.

По-видимому, чтобы вероятность ошибки синхронизации была мала, система связи должна работать с достаточно большим отношением сигнал/шум R. Поэтому одно (или два, когда $\nu \neq 0$) из этих слагаемых суммы в (7.49) будет иметь тенденцию доминировать над остальными. Это приводит к совместной оценке максимального правдоподобия метки и символов, при которой, следовательно, используется для решения следующая сумма:

$$z_\nu \triangleq \sum_l z_{\nu l} \triangleq \sum_l \max_{j_e} z_{\nu l}(j_l). \tag{7.50}$$

Так же, как и в предыдущих параграфах, можно оценить число наблюдаемых, необходимых для решения, требуя, чтобы отношение

$$r^2 = \min_\nu \frac{E^2(z_0 - z_\nu \mid 0)}{\operatorname{var}(z_0 - z_\nu \mid 0)} \tag{7.51}$$

было порядка $2k_N \log_e(1/P_e)$. Положив $y(t) = \sqrt{2}A \sin\omega_r(t - lT_s) + n(t)$; $lT_s < t < (l+1)T_s$ и $y(t) = \sqrt{2}A \sin\omega_s[t - (l+1)T_s] + n(t)$; $(l+1)T_s < t < (l+2)T_s$ и пренебрегая членами с удвоенной частотой, получим

$$z_{\nu l}(j) = (-1)^{k_r} \frac{N-\nu}{N} \frac{\cos\frac{\omega_r + \omega_j}{2}(N-\nu)\Delta T \sin\frac{\omega_r - \omega_j}{2}(N-\nu)\Delta T}{\frac{\omega_r - \omega_j}{2}(N-\nu)\Delta T} +$$

$$+ (-1)^{k_j} \frac{\nu}{N} \frac{\cos\frac{\omega_s + \omega_j}{2}\nu\Delta T \sin\frac{\omega_s - \omega_j}{2}\nu\Delta T}{\frac{\omega_s - \omega_j}{2}\nu\Delta T} + n_j. \tag{7.52}$$

где

$$n_j = \frac{1}{AT_s} \int\limits_{lT_s + \nu\Delta T}^{(l+1)T_s + \nu\Delta T} \sqrt{2}\, n(t) \sin\omega_j (t - lT_s - \nu\Delta T)\, dt.$$

Рассмотрим вначале частный случай, когда $k_j = 2N(k+j)$, где k — некоторое произвольное целое число. Конечно, при этом частоты разделены гораздо большим интервалом, чем это требуется для простой ортогональности. Существуют случаи, в которых такое условие является весьма желательным. В любом случае это ограничение даст возможность исследовать синхронизуемость ЧТ сигналов в более общих условиях. Когда $k_j = 2N(k+j)$, имеем

$$z_{\nu l}(j) = \left(1 - \frac{\nu\Delta T}{T_s}\right)\delta_{rj} + \frac{\nu\Delta T}{T_s}\delta_{sj} + n_j, \tag{7.53}$$

где δ_{ij} — символ Кронекера:

$$\delta_{ij} = \begin{cases} 1, & i = j; \\ 0, & i \neq j. \end{cases}$$

Дальнейшее упрощение достигается в предположении, что отношение сигнал/шум достаточно велико, так что наибольший выходной сигнал с большой вероятностью появляется на выходе того коррелятора, который имеет наибольшее *математическое ожидание* выходного сигнала. При этом предположении, если $\nu \leqslant N/2$ и если применима ф-ла (7.53), числитель в (7.51) равен

$$M^2\left(\frac{n-1}{n}\right)^2 \frac{\nu^2}{N^2}, \tag{7.54}$$

а знаменатель —

$$M \frac{\nu}{N} \frac{n-1}{n}\left[\frac{1}{R}+\frac{1}{n} \frac{\nu^2}{N}\right], \tag{7.55}$$

когда метки проверяются одновременно, и

$$M\left[\frac{1}{R}+\frac{n-1}{n^2}\left(\frac{\nu}{R}\right)^2\right], \tag{7.56}$$

когда они проверяются поочередно. (Последовательные символы предполагаются независимыми и равномерно распределенными; если $\nu > N/2$ по модулю N, то ν в этих выражениях следует заменить на $N-\nu$.) Наихудший случай опять возникает при $\nu = 1$ (или $N-1$), так что число символов, необходимых для решения при параллельном наблюдении,

$$M_T \approx 2\kappa_N \log_e \frac{1}{P_e}\left[\frac{N}{R}\left(\frac{n}{n-1}\right)+\frac{1}{n-1}\right]. \tag{7.57}$$

Аналогично в случае поочередного поиска с фиксированным объемом выборки общее число символов, которое нужно наблюдать,

$$M_T \approx 2\kappa''_N \log_e \frac{1}{P_e}\left[\left(\frac{n}{n-1}\right)^2 \frac{N^3}{R}+\frac{N}{n-1}\right]. \tag{7.58}$$

Порядок величины характеристики, получающейся при этом подходе, следовательно, тот же, что и в случае синхронизаторов для АИМ и ФТ, рассмотренных выше. (Слагаемые $1/R^2$ здесь отсутствуют, так как мы начали с предположения о том, что отношение сигнал/шум R велико.) Другие методы, рассмотренные в предыдущих параграфах (оценивание, оптимальное задержанное решение и т. д.), также применимы здесь и приводят, как легко проверить, к той же самой сравнительной характеристике, как и отмеченная выше.

Те же заключения справедливы для синхронизатора для фазовонекогерентной ЧТ при больших отношениях сигнал/шум. Если совместное решение максимального правдоподобия выносится относительно принимаемого символа и его фазы, то получающийся синхронизатор выносит решение, используя функцию [см. (7.9)]

$$\log_e \prod_l \max_{j_l,\, \Phi_l} \exp\left\{2R\left(a_{j_l}(\nu)\cos\Phi_l + b_{j_l}(\nu)\sin\Phi_2\right)\right\} =$$

$$= 2R \sum_l \max_{j_l}\left(a^2_{j_l}(\nu)+b^2_{j_l}(\nu)\right)^{1/2} \triangleq 2R\,\zeta_\nu, \tag{7.59}$$

где

$$\left.\begin{matrix} a_{j_l}(\nu) \\ \\ b_{j_l}(\nu) \end{matrix}\right\} = \frac{1}{AT_s} \int\limits_{lT_s+\nu\Delta T}^{(l+1)\,T_s+\nu\Delta T} y(t)\sqrt{2} \left\{\begin{matrix} \sin\omega_j(t-\nu\Delta T) \\ \\ \cos\omega_j(t-\nu\Delta T) \end{matrix}\right\} dt.$$

[То же самое выражение получается, если использовать приближение при большом отношении сигнал/шум к синхронизатору, описываемому функцией (7.8).] Такое устройство может быть реализовано, например, как параллельное соединение фазовонекогерентных согласованных фильтров, каждый из которых настроен на одну из частот $\omega_i/2\pi$ и за каждым из которых включен детектор огибающей (ср. с § 4.3).

В предположении большого отношения сигнал/шум математическое ожидание величины выходного сигнала любого детектора огибающей и дисперсия этого сигнала приближенно равны аналогичным величинам на выходе соответствующего фазовокогерентного согласованного фильтра [ср. с (3.59)]. Аналогично характеристика синхронизатора для фазовонекогерентной ЧТ почти совпадает с характеристикой фазовокогерентного синхронизатора, описанного в предыдущих абзацах при тех же самых предположениях.

Следует подчеркнуть, что эти рассуждения использовали предположение, что детектор с наибольшим математическим ожиданием выхода будет с большой вероятностью детектором с наибольшим выходом. Для величин ν, близких к нулю или N, это предположение равносильно требованию малости вероятности ошибки синхронизации. Однако, когда ν близко к $N/2$, два обстоятельства изменяют эту ситуацию: 1) существуют не один, а два (или более) детектора, имеющих относительно большие математические ожидания выходов [см. (7.53)]; 2) увеличивается вероятность того, что выход одного из детекторов с нулевым математическим ожиданием на самом деле превысит выход другого, который имеет ненулевое математическое ожидание. Оба этих обстоятельства приводят к тому, что математическое ожидание величины максимального выхода смещается и становится больше наибольшего из математических ожиданий этих выходов. Такое смещение приводит к уменьшению надежности, с которой некоторые из меток могут быть отвергнуты. Это сильно не изменяет время поиска при параллельном поиске или поочередном поиске с фиксированным объемом выборки, так как они должны быть достаточно продолжительными, чтобы надежно отвергнуть наиболее трудную метку (которая все еще будет, по-видимому, меткой $\nu=1$), независимо от того, какая метка наблюдается на самом деле. Процедуры поиска, которые приводят к экономии за счет того, что одни метки могут быть более легко отвергнуты, чем другие, теряют, однако, свою эффективность, когда принимается во внимание это смещение.

Те же замечания справедливы (и даже с более сильными ограничениями на отношение сигнал/шум), когда целые числа k_j [см. (7.48)] не обязательно имеют вид $k_j=2N(k+j)$. В этом случае абсолютная величина математического ожидания выхода j-го (фазовокогерентного) детектора ограничена [см. (7.52)] величиной

$$\frac{N-\nu}{N}\left|\frac{\sin\frac{\omega_r-\omega_j}{2}(N-\nu)\Delta T}{\frac{\omega_r-\omega_j}{2}(N-\nu)\Delta T}\right|+\frac{\nu}{N}\left|\frac{\sin\frac{\omega_s-\omega_j}{2}\nu\Delta T}{\frac{\omega_s-\omega_j}{2}\nu\Delta T}\right|\leqslant 1, \qquad (7.60)$$

где строгое неравенство имеет место для всех $\nu\neq 0$, кроме случая, когда $j=r=s$. Поэтому для достаточно больших отношений сигнал/шум нулевая метка может еще быть опознана среди всех других меток. Теперь, однако, в силу того, что несколько детекторов будут иметь ненулевые математические ожидания выходов, характеристика этой схемы синхронизации будет ухудшаться еще быстрее с уменьшением отношения сигнал/шум. Хотя эту характеристику можно оценить, удовлетворимся здесь приведенными выше замечаниями относительно качественного поведения методов синхронизации ортогональных ЧТ сигналов. Как было уже отмечено, для случаев, когда синхронизация должна быть установлена на основе свойств самих символов, существуют гораздо более эффективные множества ортогональных символов. Они детально будут рассмотрены в последующих главах.

Синхронизация ВИМ символов. Рассматриваемое множество символов состоит из сигналов вида

$$x_i(t)=\sqrt{2n}\,A\sin\omega_c t;\quad \frac{(i-1)T_s}{n}<t<\frac{iT_s}{n},$$

$$i=1,\ 2,\ \cdot\ \cdot\ \cdot,n, \qquad (7.61)$$

где $\omega_c=2\pi kn/T_s$ для некоторого целого k. Каждый символ имеет длительность T_s секунд, в то время как интервал, на котором амплитуда не равна нулю (будем называть его *подсимвольным* интервалом), равен T_s/n секунд. Одна из стратегий при синхронизации состоит, поэтому, во-первых, в сведении задачи к идентификации n меток, у которых амплитуда символа может измениться от нуля до ненулевого значения или наоборот. Во-вторых, нужно затем определить, какая из этих n оставшихся меток является в действительности правильной меткой символа.

Если ограничения на оборудование не исключают такой возможности, то, конечно, быстрейшей процедурой является та, которая объединяет обе операции. Тем не менее, так как среди этих двух подходов двухэтапная стратегия, очевидно, лучше с практической точки зрения, рассмотрение будет ограничено задачей идентификации подсимвольных меток, т. е. установлением подсимвольной синхронизации. Второй этап процедуры здесь не будет рассматриваться, так как он принадлежит к классу задач, которые рассматриваются в гл. 14.

Для того чтобы определить вид подсимвольного синхронизатора максимального правдоподобия, будем трактовать подсимволы так, как будто они сами являются символами. Поступая так, будем пренебрегать зависимостью между последовательными подсимволами. Тогда информация, которую получит синхронизатор, состоит в том, что l-й принимаемый подсимвол имеет вид:

$$y(t) = \alpha_l \sqrt{2n}\, A \sin \omega_c (t - \nu\Delta T) + n(t);$$

$$l\,\frac{T_s}{n} + \nu\Delta T < t < (l+1)\,\frac{T_s}{n} + \nu\Delta T, \tag{7.62}$$

где $n(t)$ — белый гауссовский шум. Плотность распределения случайной величины α_l имеет вид

$$p(\alpha_l) = \frac{1}{n}\,\delta(\alpha_l - 1) + \frac{n-1}{n}\,\delta(\alpha_l), \tag{7.63}$$

где $\delta(x)$ — дельта-функция Дирака. Синхронизатор максимального правдоподобия (7.3) определяет максимум по ν $[\nu = 0, 1, \ldots$ $\ldots, (N/n) - 1]$ функции

$$\prod_l \int_{-\infty}^{\infty} \exp\left[2Rz_{\nu l}\,\alpha_l - R\,\alpha_l^2\right] p(\alpha_l)\, d\,\alpha_l, \tag{7.64}$$

где

$$z_{\nu l} = \frac{1}{AT_s} \int_{l\,(T_s/n)+\nu\Delta T}^{(l+1)\,(T_s/n)+\nu\Delta T} y(t)\sqrt{2n}\,\sin\omega_c (t - \nu\Delta T)\, dt$$

и, конечно, $R = A^2T_s/N_0$. Используя равенство (7.63) и производя интегрирование, получаем требуемую статистику

$$\prod_l \left[\frac{n-1}{n} + \frac{1}{n}\, e^{2R\,(z_{\nu l} - 1/2)}\right] = \prod_l \left\{\frac{1}{n}\left[e^{2R\,(z_{\nu l} - 1/2)} - 1\right] + 1\right\}. \tag{7.65}$$

Если n и R велики по сравнению с единицей и если вновь R должно быть порядка $\log_2 n$ для того, чтобы вероятность ошибки была малой, то величины $z_{\nu l}$ являются существенными (при рассмотрении синхронизатора) только тогда, когда они превышают 1/2. Отсюда получаем, что нужно вначале принять решение относительно того, имеется ли вообще подсимвол или нет, прежде чем использовать соответствующую статистику при принятии решения относительно метки. Если, например, нужно вынести совместное решение максимального правдоподобия относительно метки и подсимвола, то синхронизатор должен определить значение ν, которое максимизирует выражение

$$\prod_l \max_{\alpha_l} \exp\left[2Rz_{\nu l}\,\alpha_l - R\,\alpha_l^2\right] = \prod_{l\in L} \exp\left[2R\left(z_{\nu l} - \frac{1}{2}\right)\right], \tag{7.66}$$

где L — множество подстрочных индексов l, для которых $z_{\nu l} > 1/2$. Если вместо этого выносится решение относительно наличия или отсутствия подсимвола на основе апостериорной вероятности этого события, то получается то же самое выражение, но L следует определить так, чтобы в него входили лишь те подстрочные индексы, для которых $z_{\nu l} \geqslant \frac{1}{2} + (1/2R)\log_e(n-1)$. В любом случае решение может быть основано на использовании множества статистик вида

$$z_\nu = \sum_{l \in L} \left(z_{\nu l} - \frac{1}{2} \right). \tag{7.67}$$

Если вероятность ошибки синхронизации мала, то величина $z_{\nu l}$, вообще говоря, не будет вносить вклад в сумму z_ν, кроме случая, когда на самом деле имеет место ненулевой подсимвольный импульс. При этом предположении число символов, требуемых для решения, как легко видеть, будет, по существу, равно тому числу, которое необходимо для определения правильной метки среди N/n конкурирующих меток, когда импульс длительностью T_s передается каждые T_s секунд по отдельному синхроканалу (что обсуждалось в гл. 6). Аналогичные утверждения справедливы при тех же самых условиях для синхронизаторов фазовонекогерентной ВИМ.

7.6. Синхронизаторы, отслеживающие символы

Предыдущие рассмотрения касались первоначального определения метки символа. Так как для всех предложенных для этого схем неявно подразумевалось, что период принимаемых символов известен, то либо этот период должен быть весьма стабильным, либо отсчет времени на приемнике должен следовать отсчету на передатчике (ср. с гл. 6). В последнем случае, в частности, синхронизация символов заканчивается, в принципе, правильным опознанием метки символа; любые последующие флуктуации метки символа будут отражены отсчетом времени в приемнике. Тем не менее часто выгодно иметь возможность прямо отслеживать изменения метки символа, не используя вспомогательный отсчет времени. Эта задача и рассматривается ниже.

Решение максимального правдоподобия относительно метки символа $\tau \triangleq \nu\Delta T$ при заданном наблюдении $y(t)$, как было показано в § 7.2, основывается на плотностях распределения, имеющих следующий типичный вид:

$$p[y_l(t)\,|\,\tau] = K\left(\sum_{j=1}^{n} \exp\left\{\frac{1}{N_0}\int_{lT_s+\tau}^{(l+1)T_s+\tau} 2y(u)\,x_j(u-\tau) - x_j^2(u-\tau)]\,du\right\} P(j)\right). \tag{7.68}$$

Приемники меток, описанные в предыдущих параграфах этой главы, находили максимум по τ функции:

$$p[y(t)\,|\,\tau] = \prod_{l=0}^{M-1} p[y_l(t)\,|\,\tau]. \tag{7.69}$$

Другой возможностью, которая рассматривается в этом параграфе, является использование взвешенной суммы производных

$$\partial \log_e [y_l(t) \mid \tau]/\partial \tau \tag{7.70}$$

для управления текущей оценкой величины τ. Так как это выражение равно нулю, когда τ равно правильной метке символа τ_0, и так как оно является монотонно убывающей функцией τ в окрестности $\tau=\tau_0$, то устройство с обратной связью, которое рассматривалось в гл. 5, способно обеспечить сходимость τ к оценке максимального правдоподобия величины τ_0 (ср. с § 5.4). Описание и анализ таких устройств отслеживания символов являются предметом этого параграфа. Начнем с когерентной АИМ и бифазной ФТ.

Когерентная АИМ и бифазная ФТ. Функция $\log_e p(y_l(t) \mid \tau)$ была аппроксимирована в § 7.3 выражением

$$Ka_l^2(\tau) = K\left[\frac{1}{AT_s}\int\limits_{lT_s+\tau}^{(l+1)T_s+\tau} y(u)\sqrt{2}\sin(\omega_c u+\Phi)\,du\right]^2 \overset{\Delta}{=} Kz[(l+1)T_s+\tau]. \tag{7.71}$$

Отсюда следует, что производную $\partial \log_e p[y_l(t) \mid \tau]/\partial\tau$ можно аппроксимировать функцией

$$[z(t) - z(t-\Delta t)]/\Delta t. \tag{7.72}$$

Получающееся устройство отслеживания символов изображено на рис. 7.1. Выходной сигнал блока, названного «генератор сигнала», является периодической последовательностью выборок $s(t) = \sum\limits_i [\delta(t-\Delta t/2-iT_s)-\delta(t+\Delta t/2-iT_s)]$, где $\delta(t)$ — дельта-функция Дирака. Фильтр цепи взвешивает последовательные входы $z(t)-z(t-\Delta t)$, $t=\tau+l'T_s$, $l'=l, l-1, l-2, \ldots$, находя тем самым сигнал ошибки на интервале $lT_s<t<(l+1)T_s$, как обсуждалось в § 5.4. (Выражение $1/\Delta t$ включено в коэффициент усиления цепи.)

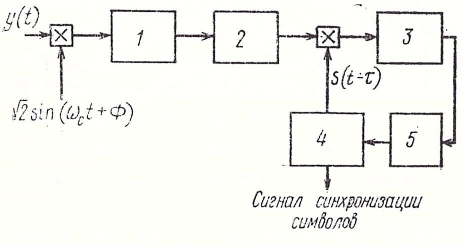


Рис. 7.1. Структурная схема синхронизатора символов, когерентная АИМ и бифазная ФТ:

1 — согласованный фильтр; *2* — квадратичное устройство; *3* — фильтр ФАПЧ; *4* — генератор сигнала; *5* — ГУН

Анализ характеристики этого устройства проводится с помощью установления его эквивалентности обобщенной системе ФАПЧ, рассмотренной в § 5.8. Как там было показано, среднеквадратическая ошибка отслеживания, связанная с таким устройством, в отсутствие каких-либо искажений, вызванных переходными фазовыми процессами или дрожанием осциллятора, является функцией лишь действующей амплитуды сигнала, спектральной плотности шума на нулевой частоте $S_n(0)$ на входе фильтра ФАПЧ (в предположении, как обычно, что ширина полосы системы ФАПЧ мала по сравнению с шириной полосы предшествующей цепи) и ширины полосы шума цепи B_L.

Сигнал 1) на входе системы ФАПЧ

$$E[z(t)] \triangleq \eta(t). \tag{7.73}$$

(Без потери общности предполагается, что $\tau_0=0$ обозначает правильную метку сигнала.) Поэтому эффективная амплитуда

$$A_e = \left| \frac{1}{2\pi} \int_0^{T_s} \eta(t)\, s'(t)\, dt \right| = \left| \frac{1}{2\pi} \int_0^{T_s} \eta'(t)\, s(t)\, dt \right| \tag{7.74}$$

(ср. с § 5.8. Так как это несущественно усложняет последующий анализ и так как получающееся обобщение имеет некоторый практический смысл, то сигнал обратной связи $s(t)$ может быть здесь любой периодической функцией t, для которой $\int_0^{T_s} s(t)\,dt=0$). Заметим, что $z(t)$ совпадает с z_ν из ф-лы (7.16), если $\nu\Delta T=\tau$ и $M=1$. Таким образом, $\eta(t)$ равняется η_ν из ф-л (7.17), (7.18) при тех же самых условиях.

Остающаяся часть входного сигнала

$$\zeta(t) = z(t) - \eta(t) \tag{7.75}$$

представляет собой шум. Поэтому шум на входе фильтра ФАПЧ имеет вид

$$n(t) = \zeta(t)\, s(t-\tau). \tag{7.76}$$

Далее

$$S_n(0) = \int_{-\infty}^{\infty} R_n(u)\, du = \sum_{i=-\infty}^{\infty} \int_0^{T_s} R_n(u+iT_s)\, du =$$

$$= \frac{1}{T_s} \sum_{i=-\infty}^{\infty} \int_0^{T_s} \int_0^{T_s} R_n(u+iT_s,\ t)\, dt\, du, \tag{7.77}$$

где $R_n(u,\ t) \triangleq E[n(t)n(t+u)]$ и где символ $E(\ldots)$ обозначает усреднение по ансамблю. Так как $R_\zeta(u,\ t) \triangleq E[\zeta(t)\zeta(t+u)]$ и $s(t)$ — периодические функции t с периодом T_s, то $S_n(0)$ может быть записано в виде

$$S_n(0) = \frac{1}{T_s} \sum_{i=-\infty}^{\infty} \int_0^{T_s} \int_0^{T_s} R_\zeta(u+iT_s,\ t)\, s(t-\tau)\, s(t+u-\tau)\, dt\, du. \tag{7.78}$$

---

1) Здесь амплитуда сигнала в любой момент времени является случайной величиной. Однако вновь, если ширина полосы цепи мала по сравнению с $1/T_s$, то выход ГУН будет определяться взвешенной суммой большого числа входных импульсов. Таким образом, для того, чтобы получить хорошую аппроксимацию сигнала на входе цепи, можно его заменить на его математическое ожидание. (*Прим. авт.*).

Сигнал $s(t)$ считался детерминированным в этом последнем преобразовании, несмотря на то, что его фаза случайно изменяется. Это справедливо, если ширина полосы системы ФАПЧ мала по сравнению с шириной полосы принимаемого сигнала (ср. с § 5.8).

Рассмотрим теперь функцию

$$\Delta^2(u,\ t) \overset{\Delta}{=} \lim_{M\to\infty} \frac{1}{M} E\left(\sum_{i=1}^{M} [\zeta(t+iT_s) - \zeta(t+u+iT_s)]\right)^2 =$$

$$= \lim_{M\to\infty} \frac{1}{M} \sum_{i=1}^{M} \sum_{j=1}^{M} \{R_\zeta[(j-i)T_s,\ t] - 2R_\zeta[u+(j-i)T_s,\ t] +$$

$$+ R_\zeta[(j-i)T_s,\ t+u] = \lim_{M\to\infty} \sum_{\nu=-(M-1)}^{M-1} \left(1 - \frac{|\nu|}{M}\right)[R_\zeta(\nu T_s,\ t) -$$

$$- 2R_\zeta(u+\nu T_s,\ t) + R_\zeta(\nu T_s,\ t+u) = \sum_{\nu=-\infty}^{\infty} [R_\zeta(\nu T_s,\ t) - 2R_\zeta(u +$$

$$+ \nu T_s,\ t) + R_\zeta(\nu T_s,\ t+u)]. \tag{7.79}$$

Это выражение справедливо тогда, когда $\lim\limits_{\nu\to\infty} R_\zeta(\nu T_s,\ t) \to 0$. Объединяя (7.78) и (7.79) и вспоминая, что $R_\zeta(\nu T_s,\ t)$ и $s(t)$ — периодические функции t и что $\int\limits_0^{T_s} s(t)dt = 0$, получаем

$$S_n(0) = -\frac{1}{2T_s} \int\limits_0^{T_s} \int\limits_0^{T_s} \Delta^2(u,\ t)\, s(t-\tau)\, s(t+u-\tau)\, dtdu. \tag{7.80}$$

Ценность этого выражения для $S_n(0)$ становится очевидной, если заметить, что

$$\Delta^2(u,\ t) = \lim_{M\to\infty} \frac{1}{M} \Delta^2_{\nu\mu}, \tag{7.81}$$

где $\Delta^2_{\nu\mu}$ определяется так же, как в (7.19) при $\nu\Delta T = t$, $\mu\Delta T = t+u$ для $0 \leqslant t \leqslant u+t \leqslant T_s$ и $\nu\Delta T = t+u-T_s$, $\mu\Delta T = t$ для $0 \leqslant t < T_s < u+t < T_s + t$. Отметим, что $\Delta^2(u,\ t)$ — периодическая функция t.

Возвращаясь к устройству отслеживания символов, изображенному на рис. 7.1, где $s(t) = \sum\limits_i [\delta(t - (\Delta t/2) - iT_s) - \delta(t + (\Delta t/2) - iT_s)]$, находим из ф-л (7.17), (7.18), что математическое ожидание сигнала ошибки на входе фильтра ФАПЧ имеет вид

$$\eta\left(t+\frac{\Delta t}{2}\right) - \eta\left(t-\frac{\Delta t}{2}\right) = \begin{cases} -2\mu_2\left(1-\dfrac{\Delta t}{T_s}\right)\dfrac{2\tau}{T_s}, & 0 \leqslant |\tau| \leqslant \dfrac{\Delta t}{2}; \\ -2\mu_2\dfrac{\Delta t}{T_s}\left(1-\dfrac{2\tau}{T_s}\right), & \dfrac{\Delta t}{2} \leqslant \tau \leqslant T_s - \dfrac{\Delta t}{2}, \end{cases} \tag{7.82}$$

где $t=\tau$ по модулю T_s. Этот сигнал изображен на рис. 7.2. Из (7.74) имеем

$$A_e = \frac{2\mu_2}{\pi T_s}\left(1 - \frac{\Delta t}{T_s}\right). \tag{7.83}$$

Согласно (7.80) получаем

$$S_n(0) = \Delta^2\left(\Delta t,\ \tau - \frac{\Delta t}{2}\right) \Big/ T_s. \tag{7.84}$$

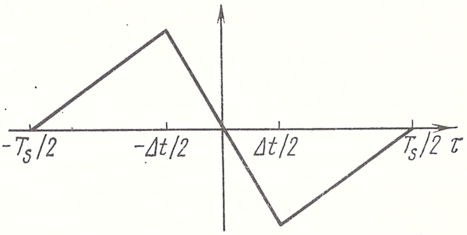


Рис. 7.2. Сигнал ошибки в синхронизаторе, изображенном на рис. 7.1, с периодической последовательностью выборок в цепи обратной связи

Хотя спектральная плотность шума зависит от момента выборки τ, она относительно медленно меняющаяся функция этого параметра. В любом случае, если система отслеживает верно, то $\tau \approx 0$ и из ф-лы (7.81) получаем

$$S_n(0) \approx \Delta^2\left(\Delta t,\ -\frac{\Delta t}{2}\right) \Big/ T_s = \frac{2\Delta t}{T_s^2}\left(1 - \frac{\Delta t}{T_s}\right)\left[\left(2 - \frac{3\Delta t}{2T_s}\right)\frac{\mu_2}{R} + \frac{1}{R^2}\right],$$

$$0 \leqslant \Delta t \leqslant \frac{T_s}{2}. \tag{7.85}$$

Наконец, среднеквадратическая ошибка отслеживания в радианах в квадрате (где 2π рад соответствуют T_s секунд) имеет вид

$$\sigma_\varphi^2 = \frac{2S_n(0)\,B_L}{A_e^2} = 2\pi^2\left(\frac{\Delta t/T_s}{1 - \Delta t/T_s}\right)\left[\left(1 - \frac{3\Delta t}{4T_s}\right)\frac{1}{\mu^2 R} + \frac{1}{2\mu_2^2 R^2}\right] \times$$

$$\times B_L T_s \underset{=}{\Delta} \left(\frac{a}{\mu_2 R} + \frac{b}{\mu_2^2 R}\right) B_L T_s. \tag{7.86}$$

Параметры a и b, как функции $\Delta t/T_s$, изображены на рис. 7.3. Вновь сталкиваемся со знакомой уже ситуацией, когда дисперсия ошибки отслеживания и линейная область сигнала ошибки прямо пропорциональны одному и тому же параметру, в данном случае Δt. Как и ранее (ср., например, с § 6.3), Δt можно оптимизировать как функцию отношения сигнал/шум системы. Так как линейная

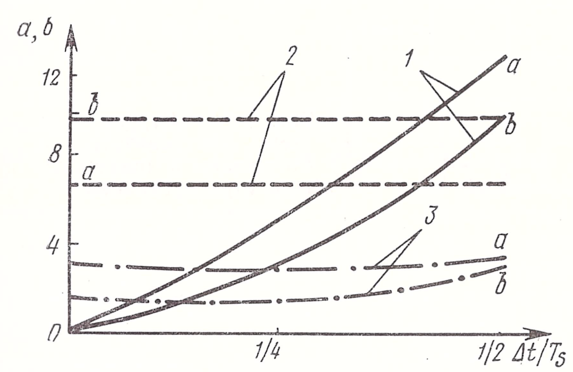


Рис. 7.3. Параметры из равенств (7.86), (7.89) и (7.95):

1 — прямоугольные импульсы; *2* — синусоидальная обратная связь; *3* — косинусоидальные импульсы область распространяется лишь на Δt-секундный интервал, то Δt не может быть сделано сколь угодно малым [по крайней мере, если нужно оставить в силе (7.86)]. Вместе с тем Δt часто может быть значительно меньше, чем $T_s/2$ секунд.

Синхронизатор символов, изображенный на рис. 7.1, также допускает несколько различных реализаций. Две из них вытекают из следующего замечания. Пусть $\alpha_l(\tau)$ обозначает интеграл

$$\alpha_l(\tau) = \frac{1}{AT_s} \int\limits_{lT_s+\tau+(\Delta t/2)}^{(l+1)\,T_s+\tau-(\Delta t/2)} \sqrt{2}\, y(t) \sin(\omega_c t + \Phi)\, dt,$$

а $\beta_l(\tau)$ обозначает интеграл

$$\beta_l(\tau) = \frac{1}{AT_s} \int\limits_{lT_s+\tau-\,(\Delta t/2)}^{lT_s+\tau+\,(\Delta t/2)} \sqrt{2}\, y(t) \sin(\omega_c t + \Phi)\, dt.$$

Сигнал ошибки на входе ГУН (рис. 7.1) также может быть выражен как взвешенная сумма вида

$$\sum_l w_l \left\{ [\alpha_l(\tau) + \beta_{l+1}(\tau)]^2 - [\alpha_l(\tau) + \beta_l(\tau)]^2 \right\} \approx$$

$$\approx \sum_l w_l \beta_l(\tau) \left[\alpha_{l-1}(\tau) - \alpha_l(\tau) \right]. \qquad (7.87)$$

Эти выражения для сигнала ошибки справедливы, если фильтр ФАПЧ имеет ширину полосы, малую по сравнению с обратной величиной периода символа T_s, т. е. если функции w_l медленно меняются в зависимости от l.

Две схемы синхронизаторов, которые получаются после этих преобразований, изображены на рис. 7.4 и 7.5. Первый из них, который называется синхронизатором *с отстающим и опережающим стробированием* (или синхронизатором *с расщепленным стробом*), представляет собой один из вариантов (возможно, самый простой) реализации более общего устройства, представленного на рис. 7.1.

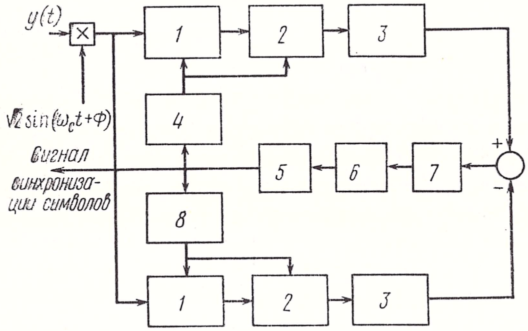
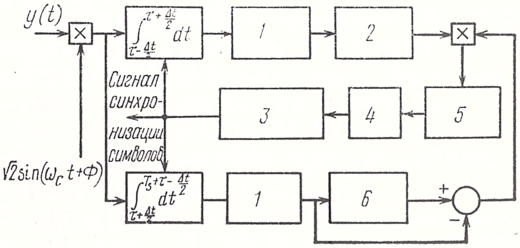

y(t)
×
1
2
3
$\sqrt{2}\sin(\omega_c t+\Phi)$
4
Сигнал синхронизации символов
5
6
7
+
−
8
1
2
3

Рис. 7.4. Структурная схема синхронизатора с отстающим и опережающим стробированием:

1 — взаимный коррелятор; *2* — выборка и запоминание; *3* — квадратичное устройство; *4* — опережение на $\Delta t/2$ с; *5* — генератор сигнала; *6* — ГУН; *7* — фильтр ФАПЧ; *8* — задержка на $\Delta t/2$ с

Модифицированный синхронизатор с отстающим и опережающим стробированием изображен на рис. 7.5. Когда система верно отслеживает $\tau \approx 0$, верхний интегратор на рис. 7.5 интегрирует по переходной области, где происходит смена символа, в то время как нижний интегратор интегрирует по интервалу, в течение которого такой переход не возникает. В случае, например, двоичной



$y(t)$
$\int_{\tau-\frac{\Delta t}{2}}^{\tau+\frac{\Delta t}{2}} dt$
1
2
Сигнал синхронизации символов
3
4
5
$\sqrt{2}\sin(\omega_c t+\Phi)$
$\int_{\tau+\frac{\Delta t}{2}}^{T_s+\tau-\frac{\Delta t}{2}} dt$
1
6
+
−

Рис. 7.5. Структурная схема модифицированного синхронизатора с отстающим и опережающим стробированием:

1 — выборка и запоминание; *2* — задержка на $(T_s - \Delta t)$, с; *3* — генератор сигнала отсчетов времени; *4* — ГУН; *5* — фильтр ФАПЧ; *6* — задержка на T_s, с

ФТ выход верхнего интегратора в идеале умножается на ноль, если не происходит переход одного символа в другой (в этом случае синхронизационной информации нет), и на знак перехода +1 или —1, если он происходит. Когда отношение сигнал/шум достаточно велико для того, чтобы можно было принимать надежные решения, это последнее толкование предлагает принимать твердые решения относительно того, имел ли место переход или нет и в соответствии с этим взвешивать интеграл в области перехода, помещая, например, идеальный ограничитель после интегратора в нижней цепи на рис. 7.5. По существу то же самое устройство получилось бы непосредственно, если бы мы с самого начала для аппроксимации статистики, определяющей синхронизатор максимального правдоподобия использовали приближение большого отношения сигнал/шум [см. (7.44)]. В случае, когда каждое решение относительно наличия и отсутствия перехода символов является правильным, дисперсия ошибки отслеживания, достижимая при использовании такого устройства, равна, как легко убедиться,

$$\sigma_\Phi^2 = 2\pi^2 \frac{\Delta t}{T_s} \frac{B_L T_s}{R}. \tag{7.88}$$

Поэтому улучшение, связанное с вынесением твердого решения, ограничено, по крайней мере, областью больших отношений сигнал/шум R. [Ср. (7.86) и (7.88); см. также задачу 7.3.] Тем не менее потенциальное упрощение при реализации этого модифицированного синхронизатора делает рассмотрение целесообразным.

Устройство отслеживания символов, изображенное на рис. 7.1, может быть использовано также с другими местными сигналами $s(t)$. Если, например, $s(t)$ — синусоида с периодом T_s, то по ф-ле (7.74) $A_e = 2\mu_2/\pi^2$, а соотношение (7.80) (когда ошибка отслеживания мала) принимает вид $S_n(0) = \frac{2T_s}{\pi^2}\left[\frac{\mu_2}{2R}\left(1+\frac{15}{4\pi^2}\right)+\frac{1}{R^2}\right]$, так что

$$\sigma_\Phi^2 = \frac{2S_n(0)\,B_L}{A_e^2} = \pi^2\left[\frac{1}{2\mu_2 R}\left(1+\frac{15}{4\pi^2}\right)+\frac{1}{\mu_2^2 R^2}\right] B_L T_s. \tag{7.89}$$

Среднеквадратическая ошибка отслеживания снова имеет вид $(a/\mu_2 R + b/\mu^2{}_2 R^2) B_L T_s$. Для сравнения эти параметры a и b также нанесены на рис. 7.3.

Хотя характеристика синхронизатора с синусоидальной обратной связью определенно хуже характеристики синхронизатора с последовательностью выборок, его более простая реализация может вполне компенсировать этот недостаток, по крайней мере, тогда, когда R достаточно велико и $B_L T_s$ достаточно мало. В частности, это верно, когда система ФАПЧ с синусоидальной обратной связью может быть заменена узкополосным фильтром, как это рассматривалось в § 6.9. Ширина полосы B_f в общем случае должна быть значительно больше ширины полосы системы ФАПЧ, которую он заменяет, но среднеквадратическая ошибка отслеживания, задаваемая теперь равенством (7.89), где B_L заменяется на B_f (по крайней мере, если $B_f \ll 1/T_s$), все еще может оставаться в допустимых границах.

Некогерентная АИМ, недвоичная ФТ и относительная когерентная ФТ. Синхронизаторы символов, описанные выше, предназначались для сигналов когерентной АИМ и двоичной ФТ. Обобщение, необходимое для того, чтобы они работали, когда используется некогерентная АИМ, недвоичная ФТ или относительная когерентная ФТ, является очевидным с точки зрения результатов, полученных в § 7.3 и 7.4.

Единственным изменением, которое необходимо внести в вышеприведенные выводы для того, чтобы приспособить их к этим типам модуляции, является изменение определения $z(t)$ в (7.71), а именно:

$$z(t) = \left[\frac{1}{AT_s}\int\limits_{t-T_s}^{t} y(u)\sqrt{2}\sin\omega_c u\,du\right]^2 + \left[\frac{1}{AT_s}\int\limits_{t-T_s}^{t} y(u)\sqrt{2}\cos\omega_c u\,du\right]^2 \tag{7.90}$$

[ср. с (7.32) и (7.41)]. С этим видоизменением рассуждения проводятся точно так же, как и раньше. Ошибка отслеживания будет такой же, как определенная ф-лами (7.86) или (7.89), с тем исключением, что коэффициент при $1/R^2$ удваивается [см. § 7.3 и 7.4 и (7.33)].

Изменения при реализации этого синхронизатора соответственно незначительны. Следует лишь заменить когерентные согласованные фильтры в рассмотренных выше синхронизаторах на некогерентные согласованные фильтры, после которых включены детекторы огибающих (ср. с § 4.3). Все остальное остается тем же. Схема синхронизатора, изображенная, например, на рис. 7.1, теперь принимает вид, изображенный на рис. 7.6.

Ортогональные символы. Методы символьной синхронизации из § 7.5 также легко приспособить для схем отслеживания символов. Рассмотрим разность $d(\tau)$ между выходом в момент $\tau + \Delta t/2$ и выходом в момент $\tau - \Delta t/2$ фильтра, согласованного с ЧТ символом или ВИМ подсимволом. Если правильная метка символа (или подсимвола) — τ_0, если $|\tau-\tau_0|<\Delta t/2$ и если символ, соответствующий рассматриваемому согласованному фильтру, был принят на самом деле, то математическое ожидание величины $d(\tau)$, как легко видеть, будет линейной функцией $\tau-\tau_0$. Величина $d(\tau)$ поэтому может быть использована как сигнал ошибки для управления моментом выборки τ. Более того, если $\tau\approx\tau_0$, то надежное решение относительно того, был ли принят этот частный символ или подсимвол, может быть построено на основе выхода фильтра в момент τ, а $d(\tau)$ можно считать сигналом ошибки только тогда, когда это решение является утвердительным.

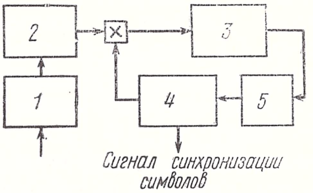


Рис. 7.6. Структурная схема синхронизатора символов, некогерентная АИМ и недвоичная ФТ:

1 — некогерентный согласованный фильтр; *2* — квадратичный детектор огибающей; *3* — фильтр ФАПЧ; *4* — генератор сигнала; *5* — ГУН

Структурные схемы получающихся устройств отслеживания изображены на рис. 7.7 для сигналов некогерентной ЧТ и на рис. 7.8 для сигналов когерентной ВИМ. Устройство, выносящее решения, определяет, какой символ был принят (в случае ЧТ), или решает, присутствовал или нет импульс подсимвола (в случае ВИМ), и в соответствии с этим стробирует сигнал ошибки. Эти схемы весьма похожи на схемы отслеживания символов для двоичной ФТ при большом отношении сигнал/шум, описанные ранее. Дисперсия ошибки отслеживания в предположении, что решения относительно наличия или отсутствия символа всегда правильны, как легко показать, будет иметь вид

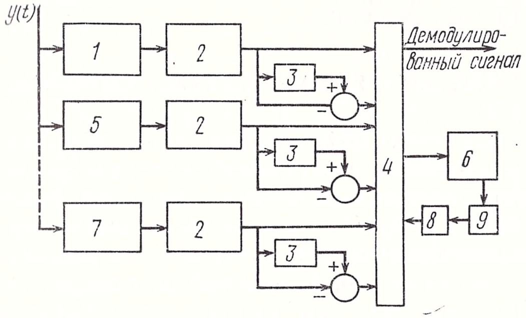


Рис. 7.7. Структурная схема синхронизатора символов ЧТ:

1 — некогерентный согласованный фильтр *1*; *2* — детектор огибающей; *3* — задержка на Δt, с; *4* — стробирующее устройство и устройство, выносящее решения; *5* — некогерентный согласованный фильтр *2*; *6*—фильтр ФАПЧ; *7* — некогерентный согласованный фильтр *n*; *8* — генератор сигнала отсчетов времени; *9* — ГУН

$$\sigma^2_{\Phi} = 4\pi^2 \frac{\Delta t}{T_s}\,\frac{B_L T_s}{pR}, \qquad (7.91)$$

где

$$p = \begin{cases} \Pr\left\{\begin{matrix}\text{два последовательных символа}\\ \text{отличаются друг от друга}\end{matrix}\right\} = \dfrac{n-1}{n}, & \text{ЧТ};\\[2ex] \Pr\left\{\begin{matrix}\text{за подсимвольным импульсом}\\ \text{не следует импульс}\end{matrix}\right\} = \dfrac{n^2-1}{n^2}, & \text{ВИМ}.\end{cases}$$

Ошибка отслеживания ЧТ импульсов определена здесь через период символа (2π рад соответствуют T_s секундам), а ошибка для ВИМ определена через период подсимвола (2π рад соответствуют T_s/n секундам).

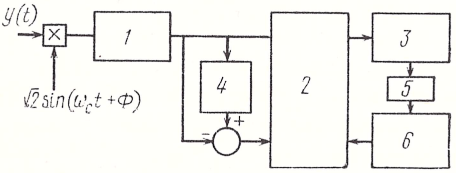


Рис. 7.8. **Структурная схема синхронизатора символов ВИМ:**

1 — фильтр, согласованный с подсимволом; 2 — стробирующее устройство и устройство, выносящее решения; 3 — фильтр ФАПЧ; 4 — задержка на Δt, с; 5 — ГУН; 6 — генератор сигнала отсчетов времени

Эта последняя схема отслеживания символов, очевидно, применима в любой импульсной системе связи. В том случае, если оценка метки символа может быть сделана достаточно точной, надежное решение, по-видимому, может быть сделано и относительно текущего принимаемого символа. После того как принимаемый символ и область перехода символов становятся известны, последняя может быть использована для уточнения оценки метки символа. Применимость этого подхода зависит от не всегда справедливого предположения об относительно большом отношении сигнал/шум и от возможности получить первоначальную оценку метки за достаточно короткий период времени.

7.7. Синхронизация непрямоугольных символов

В противоположность ситуациям, когда система находится в синхронизме, характеристика импульсной системы связи в режиме входа в синхронизм зависит от формы импульса даже тогда, когда нет ограничений на ширину полосы. Так, например, как и в гл. 6, точность отслеживания может быть увеличена (или уменьшено время поиска) сужением эффективной длительности используемых импульсов. Вместе с тем чем меньше длительность импульса, тем быстрее падает напряжение на выходе фильтра, согласованного с этим импульсом, при отклонении от момента наибольшего значения выхода. Таким образом, *требование к точности* соответственно возрастает, и ситуация, в общем, остается неизменной.

Это не означает, что тщательный выбор формы импульса не может привести к преимуществам при синхронизации. Одно потенциальное достоинство при выборе формы импульса, например, состоит в возможности упрощения аппаратуры, необходимой для синхронизации. С этой целью используется иногда модуляция *с пассивной паузой,* когда энергия передается лишь в течение части каждого периода символа. Это эквивалентно умножению символов на последовательность прямоугольных функций, один из уровней которой является нулевым (последовательность не обязательно симметричная) и, следовательно, при этом вносится частотная компонента на частоте символа, которая может быть отфильтрована или отслежена. Если, например, энергия передается лишь в течение первой половины каждого периода символа в ЧТ системе и если частоты символов достаточно разнесены, то выходы согласованных фильтров (или детекторов огибающих) на рис. 7.7 представляют собой неперекрывающиеся треугольные импульсы. Сумма этих выходов — также треугольная функция (искаженная шумом); она может быть отслежена системой ФАПЧ (или отфильтрована узкополосным фильтром) для установления требуемой символьной синхронизации; таким образом, этот метод позволяет заменить устройство, производящее выборки и выносящее решения (рис. 7.7), простым сумматором. Если не считать n-кратного увеличения уровня шума (только один выход содержит компоненту сигнала в любой момент, в то время как все n выходов содержат шум), характеристика такого устройства совпадает с характеристикой системы ФАПЧ, отслеживающей треугольный сигнал. При больших отношениях сигнал/шум n-кратное увеличение шума может быть приемлемой платой за снижение сложности аппаратуры.

Другим поводом для изменения формы импульса сигнала, используемого для целей синхронизации, является нейтрализация стохастических свойств сигнала. В рассмотрениях этой главы всюду предполагалась статистическая независимость последовательных символов; это предположение редко выполняется строго. Если в действительности последовательные символы имеют тенденцию быть одинаковыми, то число переходов символов может стать значительно меньше, чем предполагалось в вышеприведенном анализе, и характеристика синхронизатора станет значительно хуже. Вновь для решения этой задачи может быть использована модуляция с пассивной паузой. Сходный метод для случая двоичной ФТ состоит в использовании *кода Манчестера,* в котором один символ сообщения имеет вид

$$x(t) = \begin{cases} \sqrt{2}\sin\omega_c t, & 0 < t < T_s/2; \\ -\sqrt{2}\sin\omega_c t, & T_s/2 < t < T_s, \end{cases}$$

а другой символ равен $-x(t)$. Такая модификация формы символов делает характеристику синхронизатора относительно независимой от статистических свойств сигнала. За это приходится платить увеличением ширины полосы, требуемой для передачи этих модифицированных символов.

Вопрос об «оптимальном» сигнале при заданном (в этом случае) множестве требований к передаче и синхронизации, к которому неизбежно приводит рассмотрение подобного рода, здесь не ставится. Очевидно, что ответ, если его можно получить, зависит в сильной степени от наложенных ограничений. Вместе с тем влияние ошибок символьной синхронизации на характеристику всей системы связи может быть, вообще говоря, пренебрежимо малым при использовании эффективных методов синхронизации независимо от формы импульса символа. (Ср. с гл. 9.) В любом случае, следовательно, требования к синхронизации символов будут лишь незначительно влиять на проблему выбора сигнала.

Результаты этой главы также могут быть обобщены на случай непрямоугольных импульсов. Когда огибающая импульса $p(t)$, $0 \leqslant t \leqslant T_s$ произвольна, равенства (7.33) изменяются, в частности, следующим образом. Пусть

$$\lambda_i = \frac{1}{T_s} \int_0^{T_s} p(t - T_s + i\,\Delta T)\, p(t)\, dt \text{ с } \lambda_N = 1:$$

положим $\gamma_1 = \lambda_\nu$; $\gamma_2 = \lambda_{N-\nu}$; $\gamma_3 = \lambda_\mu$;

$\gamma_4 = \lambda_{N-\mu}$; $\gamma_5 = \lambda_{(\mu-\nu)}$; $\gamma_6 = \lambda_{N-(\mu-\nu)}$;

$a = \mu_4 + 4m\mu_3 + 4m^2\mu_2 - \mu_2^2$; $b = m\mu_3 + 2m^2\mu_2$ и $d = \mu_2^2 + 4m^2\mu_2$.

Тогда

$$\begin{aligned}
\eta_\nu &= \mu_2(\gamma_1^2 + \gamma_2^2) + m^2(\gamma_1 + \gamma_2)^2 + c_0/2R;\\
\sigma_{sxs}^2 &= a(\gamma_1^2 + \gamma_2^2)^2 + 8b\,\gamma_1\gamma_2(\gamma_1^2 + \gamma_2^2) + 4d\,\gamma_1^2\gamma_2^2/c_1;\\
\sigma_{sxn}^2 &= 2\mu_2(\gamma_1^2 + \gamma_2^2)/R + 2m^2(\gamma_1 + \gamma_2)^2/R;\\
\sigma_{nxn}^2 &= c_0/2R^2; \qquad\qquad (7.92)\\
\Delta_{sxs}^2 &= a[(\gamma_1^2 + \gamma_2^2) - (\gamma_3^2 + \gamma_4^2)]^2 + 8b(\gamma_1\gamma_2 - \gamma_3\gamma_4)[(\gamma_1^2 + \gamma_2^2) -\\
&- (\gamma_3^2 + \gamma_4^2)] + 4d(\gamma_1\gamma_2 - \gamma_3\gamma_4)^2/c_1;\\
\Delta_{sxn}^2 &= 2m^2[(\gamma_1 + \gamma_2)^2 + (\gamma_3 + \gamma_4)^2 - 2(\gamma_1 + \gamma_2)(\gamma_3 + \gamma_4)(\gamma_5 + \gamma_6)]/R +\\
&+ 2\mu_2[\gamma_1^2 + \gamma_2^2 + \gamma_3^2 + \gamma_4^2 - 2\gamma_1\gamma_3\gamma_6 - 2\gamma_2\gamma_4\gamma_6 - 2\gamma_2\gamma_3\gamma_5]/R;\\
\Delta_{nxn}^2 &= c_0(1 - \gamma_5^2 - \gamma_6^2)/R^2.
\end{aligned}$$

Рассуждения, использованные при рассмотрении синхронизаторов из § 7.6, применимы в равной мере в случае, когда рассматриваются импульсы любой формы, если только при этом используются согласованные с ним фильтры или взаимные корреляторы. Среднеквадратическая ошибка отслеживания, соответствующая схеме рис. 7.1, сохраняет вид

$$\sigma_\Phi^2 = 2S_n(0)\, B_L/A_e^2, \qquad (7.93)$$

где A_e и $S_n(0)$ определяются ф-лами (7.74) и (7.80) соответственно. Однако члены η_ν и $\Delta_{\mu\nu}^2$, присутствующие в этих равенствах, заменяются в соответствии с (7.92).

Как уже отмечалось, пригодность какой-либо конкретной формы импульса в сильной степени зависит от условий, в которых он будет использоваться. Одним из наиболее широко используемых непрямоугольных импульсов является так называемый *косинусоидальный* импульс, определяемый равенством [1]

$$p(t)=\sqrt{2/3}\,[1-\cos(2\pi t/T_s)],\quad 0\leqslant t\leqslant T_s. \qquad (7.94)$$

Таким образом, для того чтобы проиллюстрировать влияние формы импульса на характеристику отслеживающего синхронизатора, выберем косинусоидальный импульс в качестве практической альтернативы прямоугольному импульсу.

Рассмотрим схему синхронизатора, изображенную на рис. 7.1, где $s(t)$ — последовательность выборок $s(t)=\sum_i [\delta(t-(\Delta t/2)+iT_s)]-\delta[t+(\Delta t/2)+iT_s)]$ и где принимаемый сигнал представляет собой последовательность модулированных АИМ или ФТ косинусоидальных импульсов (т. е. $y(t)=\sqrt{2}Ax(t-iT_s)\sin(\omega_c t+\theta)+n(t)$, $iT_s<t<(i+1)T_s$, где информация содержится либо в x, либо в θ). Среднеквадратическая ошибка отслеживания опять имеет вид

$$\sigma^2_\Phi=\left(\frac{a}{\mu_2 R}+\frac{c_0 b}{\mu_2^2 R^2}\right)B_L T_s, \qquad (7.95)$$

где параметры $a=a(\Delta t/T_s)$ и $b=b(\Delta T/T_s)$ можно определить из ф-л (7.80) и (7.92). Эти зависимости также изображены на рис. 7.3. (Средняя амплитуда АИМ предполагается здесь равной нулю.) Следует отметить, что в противоположность случаю, когда импульсы прямоугольные, ошибка отслеживания, по существу, не зависит от Δt, особенно при $\Delta t<T_s/4$. Аналогично форма сигнала ошибки значительно меньше зависит от Δt. (Рис. 7.9. Амплитуда каждого

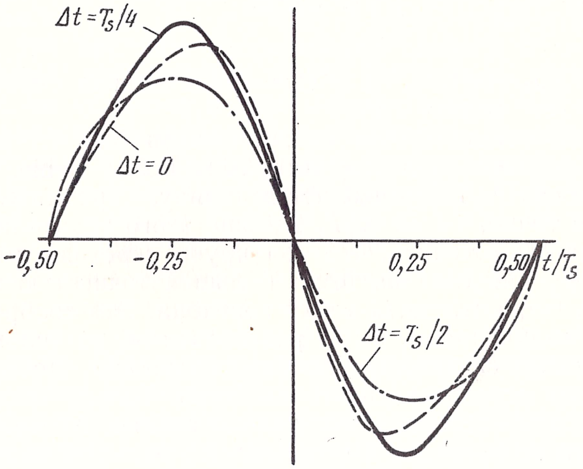


Рис. 7.9. Сигнал ошибки в синхронизаторе косинусоидальных символов

сигнала ошибки нормирована так, чтобы соответствующие уровни шума во всех случаях были одинаковыми.)

---

[1] Одним очевидным преимуществом этого импульса по сравнению с прямоугольным импульсом является его более узкий спектр (ср. с задачей 3.2). *(Прим. авт.)*.

Если форма сигнала ошибки не будет подвергаться вредным искажениям, то, по-видимому, выгодно Δt устремить к нулю в ф-ле (7.72) и построить соответствующий этому случаю синхронизатор. (На рис. 7.10 изображена более привлекательная с практической точки зрения реализация такого синхронизатора, чем та, которая представлена на рис. 7.1. Сигнал обратной связи здесь имеет вид $s(t)=\Sigma\delta(t-iT_s)$.) Среднеквадратическая ошибка отслеживания получающегося символьного синхронизатора для АИМ или ФТ может быть легко определена с помощью (7.92) и (7.93). А именно:

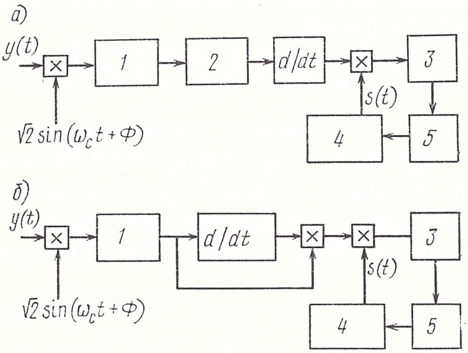


Рис. 7.10. Структурные схемы синхронизаторов символов с дифференцированием (фазовокогерентный случай):

1 — согласованный фильтр; *2* — квадратичное устройство; *3* — фильтр ФАПЧ; *4* — генератор сигнала; *5* — ГУН

$$\sigma_\Phi^2 = 2\pi^2 \left\{\frac{2}{R'} + \frac{c_0}{(R')^2}\right\} B_L \Big/ \int\limits_0^{T_s} (p'(t))^2\,dt, \qquad (7.96)$$

где $R'=A^2T_s(\mu_2+m^2)/N_0$, а $p'(t)$ — производная огибающей импульса $p(t)$ (см. задачу 7.1).

Интересно отметить, что синхронизатор рис. 7.1 способен отслеживать косинусоидальные импульсы более точно, чем прямоугольные, когда $\Delta t/T_s$ превышает величину, приближенно равную 0,1, и менее точно, когда $\Delta t/T_s$ меньше этого значения. В общем можно было бы ожидать, что чем круче переходы между последовательными импульсами, тем с большей точностью можно было бы установить и отследить точку перехода. Это соображение подкрепляется полученными выше результатами, но только в случае, когда отношение сигнал/шум достаточно велико, чтобы можно было полностью использовать это свойство. Только если отношение сигнал/шум для системы относительно велико, Δt можно выбрать малым, и это не приведет к неприемлемо большой вероятности потери синхронизма (ср. с § 6.3). И только в этом случае большая крутизна перехода между последовательными прямоугольными импульсами приносит преимущество.

Следует также отметить при обсуждении относительных достоинств прямоугольного и непрямоугольных импульсов с точки зрения синхронизации, что синхронизационная информация может быть извлечена из последовательности непрямоугольных импульсов даже в отсутствие какой-либо модуляции (ср. с задачей 7.1). Это, конечно, неверно, когда импульсы прямоугольные. В этом случае могут оказаться необходимыми ограничения на модуляцию, чтобы получить минимально необходимое число переходов и тем самым избежать возможной потери синхронизации.

7.8. Заключительные замечания

Эта глава была посвящена методам получения символьной синхронизации непосредственно по принимаемой последовательности символов, переносящих информацию. Были рассмотрены два типа синхронизаторов: задача первого состоит в определении правильной метки символа среди конечного множества меток; второго — в том, чтобы отслеживать эту метку. При исследовании синхронизаторов первого типа внимание было сосредоточено на так называемых синхронизаторах максимального правдоподобия. Было найдено, что характеристика этого класса синхронизаторов, по существу, сравнима с характеристикой, которая получается при использовании метода двух каналов, рассмотренного в гл. 6, если эффективная длительность импульса синхросигнала равна периоду символа. Но так как в методе двух каналов необходимо разделить имеющуюся мощность между каналами передачи информации и синхронизации, а здесь вся мощность одновременно используется как для передачи информации, так и для синхронизации, то одноканальный метод может оказаться эффективнее двухканального даже тогда, когда длительность синхроимпульса относительно мала.

Имеются три причины рассмотрения класса отслеживающих синхронизаторов, введенных в § 7.6. Во-первых, это достаточно общий класс, он включает в себя многие символьные синхронизаторы, представляющие практический интерес. Во-вторых, в него входят как подкласс синхронизаторы, предназначенные для решения уравнения максимального правдоподобия (ср. с § 5.4), по крайней мере, в наиболее трудном случае, когда отношение сигнал/шум R мало. Следовательно, получающаяся оценка метки символа асимптотически оптимальна в среднеквадратическом смысле (§ 2.8), когда отношение сигнал/шум для системы ФАПЧ стремится к бесконечности, т. е. когда ширина полосы системы ФАПЧ B_L стремится к нулю. (Конечно, это не гарантирует оптимальности при каком-либо другом множестве условий.)

Во-вторых, доказательство асимптотической оптимальности формулы оценки максимального правдоподобия использует определенные условия регулярности, которые не выполняются, если не наложены ограничения на несколько первых производных огибающей импульса. В реальных физических системах, конечно, ограничения на ширину полосы канала в любом случае не позволяют использовать прямоугольные импульсы, так что эта оговорка не приводит к серьезным последствиям. Выводы для прямоугольных импульсов остаются справедливыми, если такие импульсы могут быть приемлемой идеализацией реальных импульсов.

И, в-третьих, что, возможно, наиболее важно, можно получить относительно простые аналитические соотношения, связывающие среднеквадратическую ошибку отслеживания с отношением сигнал/шум на входе приемника и другими физическими параметрами.

Задачи

7.1. а) Пусть $p(t)$ — импульс произвольной формы, определенный так же, как в (7.92), и предположим, что первая и вторая производные импульса существуют и абсолютно интегрируемы на интервале $0 \leqslant t \leqslant T_s$. Показать, что если в (7.92) $\mu = \nu + 1$, то

$$\lim_{\Delta T \to 0} \frac{\Delta^2_{sxs}}{(\Delta T)^2} = 4a\left(\gamma_1\gamma_1' - \gamma_2\gamma_2'\right)^2 - 16\,b\left(\gamma_1\gamma_1' - \gamma_2\gamma_2'\right)\left(\gamma_1\gamma_2' - \gamma_2\gamma_1'\right) +$$

$$+ 4d\left(\gamma_1\gamma_2' - \gamma_2\gamma_1'\right)^2 / c_1;$$

$$\lim_{\Delta T \to 0} \frac{\Delta^2_{sxn}}{(\Delta T)^2} = \frac{2m^2}{R}\left\{\left(\gamma_1' - \gamma_2'\right)^2 - (\gamma_1 + \gamma)^2\gamma_3''\right\} + \frac{2\mu_2}{R}\left\{\left(\gamma_1'\right)^2 + \left(\gamma_2'\right)^2 -\right.$$

$$\left. - \left(\gamma_1^2 + \gamma_2^2\right)\gamma_3''\right\};$$

$$\lim_{\Delta T \to 0} \frac{\Delta^2_{nxn}}{(\Delta T)^2} = -\frac{c_0}{R^2}\gamma_3'',$$

где $\gamma(t) = \frac{1}{T_s}\int\limits_0^{T_s} p(u - T_s + t)\,p(u)\,du$; $\gamma'(t) = d\gamma(t)/dt$; $\gamma''(t) = d^2\gamma(t)/dt^2$ и подстрочные индексы 1, 2 и 3 обозначают аргументы $\tau \underset{=}{\Delta} \lim\limits_{\Delta T \to 0} \nu\Delta T$; $T_s - \tau$ и T_s соответственно.

б) Используйте этот результат, чтобы показать, что в случае достаточно большого отношения сигнал/шум, когда ошибка отслеживания мала, дисперсия ошибки отслеживания задается ф-лой (7.96). Заметьте, что при этих условиях среднеквадратическая ошибка отслеживания символов ФТ не зависит от модуляции.

7.2. В рассмотрениях, помещенных в § 7.6 и 7.7, не принималась во внимание зависимость спектральной плотности шума $S_n(0)$ на входе системы ФАПЧ от ошибки отслеживания τ [ср. с (7.84)].

а) Показать, что, когда $B_L T_s$ мало и когда дисперсия σ^2_Φ достаточно мала, чтобы оправдать линейное приближение в системе ФАПЧ, хорошей аппроксимацией служит

$$\sigma^2_\Phi = \int\limits_{-\infty}^{\infty} \sigma^2_\Phi(\tau)\,p(\tau)\,d\tau,$$

где $\sigma^2_\Phi(\tau)$ — дисперсия, получаемая теоретически, когда $S_n(0)$ оценивается в точке τ; $p(\tau) = (1/\sqrt{2\pi}\,\sigma_\tau)\exp\left(-\tau^2/2\sigma^2_\tau\right)$ при $\sigma_\tau = (T_s/2\pi)\,\sigma_\Phi$.

б) Используя этот результат, показать, что если принять во внимание зависимость $S_n(0)$ от τ, дисперсия ошибки отслеживания, задаваемая (7.86), увеличивается в

$$\left[1-\left(\frac{\mu_4}{c_1\mu_2^2}+\frac{3}{2\mu_2 R}\right)\frac{B_L T_s}{1-(\Delta t/T_s)}\right]^{-1} \text{ раз.}$$

7.3. Рассмотрим устройство отслеживания, схема которого отличается от схемы рис. 7.5 тем, что в ней после нижнего интегратора включен идеальный ограничитель.

а) Показать, что, когда огибающие принимаемых двоичных ФТ импульсов прямоугольны, дисперсия ошибки отслеживания (при линейной модели) для такого устройства равна

$$\sigma_\Phi^2 = 2\pi^2\left(\frac{\Delta t}{T_s}\right)\frac{B_L T}{(1-2p)^2 R},$$

где p обозначает вероятность ошибки определения синхросимвола при отношении сигнал/шум $R'=R[1-\Delta t/T_s]$.

б) Показать, что для малых отношений сигнал/шум R наличие идеального ограничителя увеличивает дисперсию фазовой ошибки в $\pi/2$ раз, в то время как в другом предельном случае, когда $R\to\infty$, оно уменьшает дисперсию в $[1-(\Delta t/T_s)]/[1-(\frac{3}{4}\Delta t/T_s)]$ раз.

в) Получить аналогичные результаты, когда огибающие импульсов имеют косинусоидальную, а не прямоугольную форму.

7.4. Оценить время, необходимое для установления символьной синхронизации для АИМ и ФТ непосредственно из модулированного сигнала при использовании различных поочередных методов поиска, рассмотренных в гл. 6 [ср. с (7.33)].

7.5. Показать, что, когда последовательные символы ФТ сигнала имеют статистически независимые, но не обязательно равномерно распределенные фазы, все еще можно использовать соотношение (7.92), но следует положить $m^2=E(\cos\Delta\theta_l)$; $\mu_2=1-m^2$; $a=b=0$ и $d/c_1=E(\cos^2\Delta\theta_l)+2E(\cos\Delta\theta_l\cos\Delta\theta_{l+1})-3E^2(\cos\Delta\theta_l)$, где $\Delta\theta_l=\theta_l-\theta_{l+1}$, а θ_l обозначает фазу импульса на интервале $lT_s\leqslant t\leqslant(l+1)T_s$.

Глава 8

СИНХРОНИЗАЦИЯ НЕСУЩЕЙ МЕТОДОМ МАКСИМАЛЬНОГО ПРАВДОПОДОБИЯ

8.1. Введение

Предыдущая глава была посвящена исследованию методов установления синхронизации символов непосредственно по принимаемому сообщению. В этой главе будет показано, что некоторые из этих методов применимы в равной мере к задаче получения опорной несущей (или поднесущей) из модулированной несущей. Так как фаза несущей будет неизбежно меняться во времени, то задача состоит не в проверке гипотез относительно фазы, а в отслеживании периодического сигнала, и здесь подходят методы, использованные в гл. 5.

Задача выделения опорной несущей из информационных сигналов, когда спектр модулированной несущей содержит дискретную компоненту на частоте несущей, уже была рассмотрена в гл. 6. Необходимо лишь определить отношение мощности компоненты несущей к спектральной плотности шума в этом частотном диапазоне, для того чтобы оценить точность, с которой может быть отслежена несущая. Поэтому в этой главе будут рассматриваться только каналы передачи информации, которые не имеют дискретной частотной компоненты несущей, или, по крайней мере, мощность такой компоненты не достаточна, чтобы ее можно было отследить сколь-нибудь надежно.

В первых нескольких параграфах этой главы в предположении, что известна символьная синхронизация, рассматриваются и анализируются устройства отслеживания несущей для различных типов модуляции. Так как символьная синхронизация должна быть установлена до того, как начинается демодуляция, и так как несущая отслеживается во всех режимах передачи, то это предположение полностью оправдано. В режиме входа в синхронизм символьная синхронизация может быть, а может и не быть достигнута до входа в синхронизм несущей. (Она могла бы быть установлена, например, путем использования одного из фазовонекогерентных методов гл. 7.) Если ее нет, то методы, развитые здесь, все же продолжают работать, хотя и с меньшей эффективностью. В последующих параграфах это предположение о первоначальной символьной синхронизации будет снято.

Здесь рассматривается следующая проблема. Принимаемый сигнал $y(t)$ имеет вид $y_l(t)=x_j\ (t-\tau,\ \Phi_0)+n(t)$; $\tau+lT_s<t<\tau+(l+1)T_s$; $l=\ldots, -1, 0, 1, 2, \ldots$; $j_l=1, 2, \ldots, n$, где $n(t)$ — белый гауссовский шум; Φ_0 обозначает фазу несущей, а τ — метка символа, которая вначале предполагается известной. (Поэтому без потери общности положим $\tau=0$.) Задача состоит в том, чтобы отследить фазу несущей Φ_0. Подход, который развивается здесь, аналогичен тому, который был использован в § 5.4 и 7.6, а именно, используется обратная связь для того, чтобы найти решение взвешенной суммы уравнений правдоподобия

$$\frac{\partial \log_e p\,[y_l(t)|\Phi]}{\partial \Phi}=0. \tag{8.1}$$

где

$$p\,[y_l(t)\,|\,\Phi]=K\left(\sum_{j=1}^{n}\exp\left\{\frac{1}{N_0}\int\limits_{lT_s}^{(l+1)\,T_s}[2y(t)\,x_j(t,\ \Phi)-\right.\right.$$

$$\left.\left.-x_j^2(t,\ \Phi)]\,dt\right\}P(j)\right). \qquad (8.2$$

(Это последнее равенство следует непосредственно из аналогичных результатов § 7.2.) Получающееся устройство называется *синхронизатором максимального правдоподобия для синхронизации несущей*. Это устройство оптимально в том же смысле, в котором система ФАПЧ была оптимальной для отслеживания немодулированной несущей.

Принимая этот подход максимального правдоподобия, мы, конечно, игнорируем любую информацию относительно фазы несущей, которая может быть получена с помощью предполагаемой символьной синхронизации. Это может быть оправдано либо тогда, когда фазы несущей и метки символа фактически независимы, либо тогда, когда ширина спектра сигнала мала по сравнению с его центральной частотой. В последнем случае опорную синхронизацию можно было бы рассматривать как точную с точки зрения отсчета символов, но все же она довольно груба, если ее точность сравнивать с периодом несущей. Если ни один из этих случаев не имеет места, то фактически несущая отсутствует, но ее можно рассматривать как составную часть сигнала, соответствующего символам, и применять методы гл. 7.

8.2. Синхронизация АИМ несущей

Если принимаемый сигнал имеет вид[1]: $y_l(t)=\sqrt{2}\times \times Ax_l\sin(\omega_c t+\Phi_0)+n(t);\ lT_s<t<(l+1)T_s$ (где x_l обозначает информацию, $n(t)$ — белый шум, имеющий одностороннюю спектральную плотность N_0, и Φ_0 — фазу несущей), то можно поступить так же, как в § 7.3, и показать, что хорошим приближением для функции $p[y_l(t)\,|\,\Phi]$ служит

---

[1] Огибающие импульсов здесь предполагаются прямоугольными. Однако их действительный вид не будет влиять на результаты, которые излагаются ниже, если ширина спектра получающегося сигнала будет мала по сравнению с его центральной частотой. Изменения, которые требуется внести в устройства отслеживания для того, чтобы они были пригодны для работы с непрямоугольными импульсами, очевидны. (*Прим. авт.*).

$$p\,[y_l(t)\,|\,\Phi] = K\mathrm{e}^{Ra_l^2(\Phi)}, \tag{8.3}$$

где $a_l(\Phi) = \dfrac{1}{AT_s}\displaystyle\int\limits_{lT_s}^{(l+1)\,T_s} y(t)\sqrt{2}\sin(\omega_c t + \Phi)\,dt.$

(Напомним, что равенство (8.3) является точным, когда амплитуды АИМ импульсов имеют гауссовское распределение, и, кроме того, является разумной аппроксимацией для всех отношений сигнал/шум $R = A^2T_s/N_0$ в случае других распределений.) Используя (8.3), получаем

$$\frac{\partial \log_e p\,[y_l(t)\,|\,\Phi]}{\partial \Phi} = \frac{2R}{A^2T_s^2}\int\limits_{lT_s}^{(l+1)\,T_s} y(t)\sqrt{2}\sin(\omega_c t + \Phi)\,dt \int\limits_{lT_s}^{(l+1)\,T_s} y(t)\sqrt{2}\cos(\omega_c t + \Phi)\,dt. \tag{8.4}$$

Для анализа характеристики получающегося устройства отслеживания несущей (рис. 8.1) положим, что $y_l(t) = \sqrt{2}Ax_l \times$

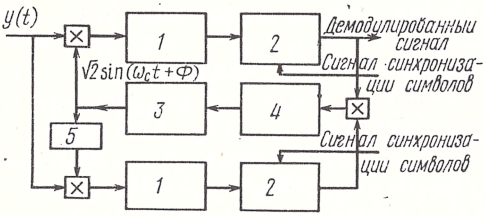

y(t)
1
2
Демодулированный сигнал
$\sqrt{2}\sin(\omega_c t+\Phi)$
Сигнал синхронизации символов
3
4
5
Сигнал синхронизации символов
1
2

Рис. 8.1. Структурная схема синхронизатора АИМ несущей:

1 — согласованный фильтр; *2* — квадратичное устройство; *3* — фильтр ФАПЧ; *4* — генератор сигнала; *5* — ГУН

$\times \sin[\omega_c t + \Phi_0(t)] + n(t)$ — принимаемый сигнал и что $z(t) = \sqrt{2} \times \sin[\omega_c t + \Phi_1(t)]$ — выход ГУН. Тогда входом фильтра ФАПЧ на интервале $(l+1)T_s < t < (l+2)T_s$ будет

$$[AT_s x_l \sin\Phi_e(l) + n_1(l)]\,[AT_s x_l \cos\Phi_e(l) + n_2(l)] = \frac{1}{2}A^2T_s^2 x_l^2 \sin 2\Phi_e(l) + AT_s x_l \sin\Phi_e(l)\, n_2(l) + AT_s x_l \cos\Phi_e(l)\, n_1(l) + n_1(l)\, n_2(l), \tag{8.5}$$

где фаза $\Phi_e(l) = \Phi_1(t) - \Phi_0(t)$; $lT_s < t < (l+1)T_s$ предполагается постоянной на каждом T_s-секундном интервале и где

$$n_1(l) = \int\limits_{lT_s}^{(l+1)\,T_s} n(t)\sqrt{2}\cos[\omega_c t + \Phi_1(t)]\,dt;$$

$$n_2(l) = \int\limits_{lT_s}^{(l+1)\,T_s} n(t)\sqrt{2}\sin[\omega_c t + \Phi_1(t)]\,dt. \tag{8.6}$$

Лишь первый член правой части (8.5) несет какую-то информацию относительно фазы принимаемого сигнала. Остальные члены описывают шум. Если ширина полосы системы ФАПЧ мала по сравнению с $1/T_s$ (и это будет, если, как мы предполагали, $\Phi_0(t)$ и, следовательно, $\Phi_1(t)$ и $\Phi_e(t)$ — медленно меняющиеся функции времени), то выход ГУН будет определяться взвешенной суммой большого числа входных импульсов. Как и в § 7.6, сигнал на входе фильтра ФАПЧ может быть аппроксимирован усреднением по x_l первого члена в правой части равенства (8.5). Поэтому эффективная амплитуда сигнала равна

$$A_e = \frac{d}{d\Phi_e}\left[\frac{1}{2} A^2 T_s^2 E(x^2) \sin 2\Phi_e\right]_{\Phi_e=0} = A^2 T_s^2 E(x^2), \tag{8.7}$$

где предполагается, что $E(x^2) \triangleq E(x^2_l)$ не зависит от l [ср. с (5.109)].

Так как шум $n(t)$ на входе устройства предполагается белым, то шумы на входе фильтра ФАПЧ, соответствующие любым двум различным интервалам: $lT_s < t < (l+1) T_s$ и $mT_s < t < (m+1) T_s$, $l \neq m$, независимы. А так как

$$E[n_1^2(l)] = E[n_2^2(l)] = \frac{N_0}{2} T_s \quad \text{и} \quad E[n_1(l) n_2(l)] = 0, \qquad \begin{matrix}(8.8)\\(8.9)\end{matrix}$$

то автокорреляционная функция шума

$$\tau = \begin{cases} \sigma_n^2\left(1 - \dfrac{|\tau|}{T_s}\right), & |\tau| \leqslant T_s; \\ 0, & |\tau| > T_s, \end{cases} \tag{8.10}$$

где

$$\sigma_n^2 = E\{AT_s x_l \sin\Phi_e(l)\, n_2(l) + AT_s x_l \cos\Phi_e(l)\, n_1(l) +$$

$$+ n_1(l)\, n_2(l)\}^2 = A^2 T_s^2 E(x^2) \frac{N_0}{2} T_s + \left(\frac{N_0}{2}\right)^2 T_s^2.$$

Таким образом,

$$S_n(\omega) = \sigma_n^2 \int_{-T_s}^{T_s} \left(1 - \frac{|\tau|}{T_s}\right) e^{-i\omega\tau}\, d\tau = \sigma_n^2 T_s \left(\frac{\sin\dfrac{\omega T_s}{2}}{\dfrac{\omega T_s}{2}}\right)^2. \tag{8.11}$$

Как и в случае обычной системы ФАПЧ, схема устройства отслеживания, изображенная на рис. 8.1, теперь хорошо аппроксимируется при малых ошибках отслеживания линейной схемой, изображенной на рис. 8.2. Ширина полосы шума $n'(t)$ порядка $1/T_s$, и так как ширина полосы системы ФАПЧ предполагается малой по сравнению с этой величиной, шум, по существу, является белым с двусторонней спектральной плотностью $S_n(0) = \sigma^2_n T_s$. Таким образом, здесь снова применимы результаты § 5.6. Дисперсия фазовой ошибки, обусловленная шумом на входе, равна

$$\sigma_\Phi^2 \approx 2S_n(0)\, B_L / A_e^2 = B_L T_s (1/R' + 1/2R'^2), \tag{8.12}$$

где $R'=A^2E(x^2)T_s/N_0$ — отношение средней энергии сигнала к спектральной плотности аддитивного шума, а B_L — ширина полосы шума эквивалентной системы ФАПЧ, изображенной на рис. 8.2.

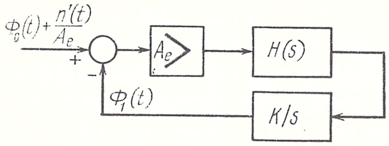


Рис. 8.2. Функциональная схема линейной модели синхронизатора, изображенного на рис. 8.1

Следует отметить, что сигнал на выходе отслеживающего устройства, изображенного на рис. 8.1, может быть либо в фазе с принимаемой несущей, либо отличаться по фазе на 180°. Эта неоднозначность в 180° неизбежна; очевидно, что устройство отслеживания несущей не позволяет при отсутствии абсолютной опорной несущей различить сигналы $\sqrt{2}Ax\sin(\omega_c t+\Phi_0)$ и $\sqrt{2}A(-x)\times\sin(\omega_c t+\Phi_0+\pi)$. Конечно, существует несколько способов разрешения этой неоднозначности. В общем случае либо естественная избыточность информационной последовательности, либо избыточность, преднамеренно вносимая для исправления ошибок синхронизации кадров или других целей, будут достаточны для того, чтобы дать возможность получателю различить правильное сообщение и обратное к нему. В любом случае, хотя такие неоднозначности сразу же вызывают беспокойство, они редко приводят к серьезным последствиям.

8.3. Отслеживание фазы ФТ несущей

Пусть теперь принимаемый сигнал представляет собой ФТ синусоиду, искаженную шумом $y_l(t)=\sqrt{2}A\sin[\omega_c t+\theta_j{}^l+\Phi_0(t)]+n(t)$; $lT_s<t<(l+1)T_s$, где $\theta_j=2\pi j/n$, $j=1, 2, \ldots, n$ — фаза, содержащая информацию, а $\Phi_0(t)$ — фаза, которая должна быть отслежена. С первого взгляда может показаться бессмысленной попытка отслеживать $\Phi_0(t)$, когда θ_{j_l} также случайная величина. Однако, если местная опорная фаза абсолютно стабильна, то Φ_0 равна нулю и θ_{j_l} может принимать лишь одно из n точно известных значений. Нестабильность опорной фазы вызывает расхождение между значениями, которые, по предположению, могут принимать фазы θ_{jl}, и значениями, которые они фактически принимают. Другими словами, $\Phi_0(t)$ приводит просто к смещению наблюдаемых фаз. Если $\Phi_0(t)$ медленно меняется со временем, оставаясь приближенно постоянной на ряде T_s-секундных интервалов, то это смещение, по-видимому, может быть отслежено.

Функция $p[y_l(t)\,|\,\Phi]$ может быть здесь выражена в виде (ср. с § 7.4)

$$p[y_l(t)\,|\,\Phi]=\frac{K}{n}\sum_{j=1}^{n}\exp\{2R[a_l(\Phi)\cos\theta_j+b_l(\Phi)\sin\theta_j]\}, \qquad (8.13)$$

где

$$\left.\begin{matrix} a_l(\Phi) \\ \\ b_l(\Phi) \end{matrix}\right\} = \frac{1}{AT_s}\int\limits_{lT_s}^{(l+1)T_s} y(t)\sqrt{2}\left\{\begin{matrix}\sin(\omega_c t+\Phi) \\ \\ \cos(\omega_c t+\Phi)\end{matrix}\right\} dt.$$

Оценка максимального правдоподобия величины Φ при заданном $y_l(t)$, $lT_s<t<(l+1)T_s$ является решением уравнения

$$\partial \log_e p\,[y_l(t)\,|\,\Phi]/\partial\Phi = 0. \tag{8.14}$$

Заметим, однако, что любая величина $\Phi=\hat{\Phi}$, удовлетворяющая уравнению

$$\frac{d}{d\Phi}\sum_{j=1}^{n}[a_l(\Phi)\cos\theta_j + b_l(\Phi)\sin\theta_j]^n = 0, \tag{8.15}$$

также будет решением ур-ния (8.14).

Для того чтобы доказать это утверждение, вначале разложим экспоненты из (8.13) в степенные ряды, возьмем логарифм получающегося выражения и после дифференцирования по Φ получим

$$\frac{\partial \log_e p\,[y_l(t)\,|\,\Phi]}{\partial\Phi} = \frac{\dfrac{K}{n}\displaystyle\sum_{\nu=0}^{\infty}\frac{(2R)^\nu}{\nu!}\,\frac{dF_\nu(\Phi)}{d\Phi}}{p\,(y_l(t)\,|\,\Phi]}, \tag{8.16}$$

где $F_\nu(\Phi) = \sum\limits_{j=1}^{n}[a_l(\Phi)\cos\theta_j + b_l(\Phi)\sin\theta_j]^\nu = \sum\limits_{j=1}^{n}[c_l(\Phi)\,e^{i\theta_j} + c_l^*(\Phi)\times$ $\times\, e^{-i\theta_j}]^\nu$; $c_l(\Phi)\,\underset{=}{\Delta}\,[a_l(\Phi)-i\,b_l(\Phi)]/2$, а $c_l^*(\Phi)$ комплексно-сопряженная величина. Используя биномиальные разложения для отдельных слагаемых, меняя порядок суммирования и замечая, что

$$\sum_{j=1}^{n} e^{i\theta_j\mu} = \begin{cases} 0, & \mu\neq 0\,(\mathrm{mod}\,n); \\ n, & \mu = 0\,(\mathrm{mod}\,n). \end{cases}$$

получим

$$F_\nu(\Phi) = n\binom{\nu}{\frac{\nu}{2}}|c_l(\Phi)|^\nu + n\sum_{\mu=1}^{[\nu/n]}\binom{\nu}{\frac{\nu-\mu n}{2}}\left\{[c_l(\Phi)]^{\mu n} + [c_l^*(\Phi)]^{\mu n}\right\}, \tag{8.17}$$

где $[\nu/n]$ обозначает наибольшее целое число, не превосходящее ν/n, а биномиальные коэффициенты $\binom{\nu}{j}$ полагаются равными нулю, если j не является целым числом. Но, как легко проверить, $|c_l(\Phi)|$ не зависит от Φ и

$$\frac{d}{d\Phi}F_\nu(\Phi) = i\,n^2\sum_{\mu=1}^{[\nu/n]}\mu\binom{\nu}{\frac{\nu-\mu n}{2}}\left\{[c_l(\Phi)]^{\mu n} - [c_l^*(\Phi)]^{\mu n}\right\}. \tag{8.18}$$

Эта сумма, очевидно, равна нулю, если $c^n{}_l(\Phi)=[c^*{}_l(\Phi)]^n$, т. е. если $(d/d\Phi)F_\nu(\Phi)=0$ для $\nu=n$. Таким образом, если

$$\frac{d}{d\Phi}F_n(\Phi)=\frac{n^2}{2^{n-1}}\sum_{\substack{\nu=1\\ \nu\text{—нечетные}}}^{n}(-1)^{(\nu-1)/2}\binom{n}{\nu}a_l^{n-\nu}(\Phi)\,b_l^{\nu}(\Phi)=0, \tag{8.19}$$

то числитель (8.16) равен нулю, и уравнение правдоподобия удовлетворяется, что требовалось доказать.

Если на интервале $lT_s<t<(l+1)T_s$ принимается сигнал $y_l(t)=\sqrt{2}AT_s\sin(\omega_c t+\theta_r+\Phi_0)+n(t)$, то

$$\left.\begin{aligned} a_l(\Phi)&=\cos\Phi'+n_1;\\ b_l(\Phi)&=\sin\Phi'+n_2,\end{aligned}\right\} \tag{8.20}$$

где $\Phi'=\Phi_0-\Phi+\theta_r\triangleq\Phi_e+\theta_r$ и

$$\left.\begin{matrix} n_1\\ \\ n_2\end{matrix}\right\}=\frac{1}{AT_s}\int_{lT_s}^{(l+1)T_s}n(t)\sqrt{2}\left\{\begin{matrix}\sin(\omega_c t+\Phi)\\ \\ \cos(\omega_c t+\Phi)\end{matrix}\right\}dt.$$

Таким образом, $c_l(\Phi)=(e^{-i\Phi'}/2)+m_1$; $c^*{}_l(\Phi)=(e^{i\Phi'}/2)+m_2$, где $m_1=(n_1-in_2)/2$; $m_2=m^*{}_1$ и

$$in^2E\{c_l^n(\Phi)-[c_l^*(\Phi)]^n\}=\frac{n^2}{2^{n-1}}\sin n\Phi'=\frac{n^2}{2^{n-1}}\sin n\Phi_e. \tag{8.21}$$

Из равенства (8.21) следует, что один из корней функции, стоящей в левой части (8.15), в действительности представляет собой несмещенную оценку величины Φ_0. Кроме того, знак математического ожидания этой функции будет положительным, когда оценка Φ величины Φ_0 меньше, чем Φ_0, и отрицательным, когда Φ превышает Φ_0 при $|\Phi_0-\Phi|\leqslant\pi/n$. В соответствии с этим, если как вход для ГУН использовать саму эту функцию после соответствующей фильтрации, то получающееся в результате устройство будет способно отслеживать фазу принимаемой несущей. Эти системы отслеживания фазы ФТ несущей показаны на рис. 8.3 для $n=2$, 3 и 4.

Имеются, конечно, $2n-1$ других значений Φ_e, для которых математическое ожидание (8.15) равно нулю. Математическое ожидание второй производной этого уравнения отрицательно для $n-1$ из его решений; они определяют все n возможных точек захвата. То же самое будет, если используется формула оценки максимального правдоподобия, поскольку, как уже было показано, любое решение (8.15) является также решением уравнения максимального правдоподобия. На самом деле эта n-кратная неопределенность, очевидно, является неизбежной, если несущую нужно выделить непосредственно из модулированного сигнала[1].

---

[1] Сюда в равной мере относятся те замечания, которые были сделаны относительно аналогичной задачи в предыдущем параграфе. Имеется еще другой метод решения этой задачи для дискретных систем; он состоит в разностном кодировании информации, т. е. в представлении информации в виде изменений между соседними символами, а не с помощью самих символов (ср. с § 12.6). *(Прим. авт.)*.

Эти цепи отслеживания несущей являются подоптимальными только вследствие того, что математические ожидания производных в ур-ниях (8.14) и (8.15) не обязательно равны. Поэтому

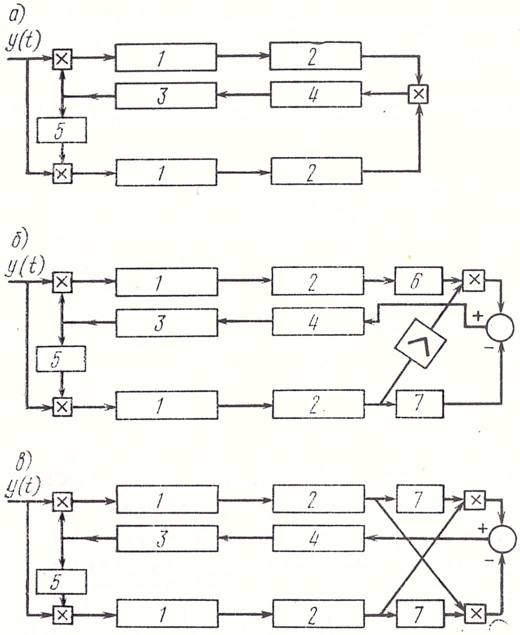


Рис. 8.3. Структурные схемы синхронизаторов ФТ несущей:
а) бифазный случай; *б)* трехфазный случай; *в)* четырехфазный случай

1 — согласованный фильтр; *2* — выборка и запоминание; *3* — ГУН; *4* — фильтр ФАПЧ; *5* — поворот фазы на 90°; *6* — возведение в квадрат; *7* — возведение в куб

действительная оценка максимального правдоподобия могла бы иметь меньшую дисперсию. Тем не менее, когда отношение сигнал/шум $R=A^2T_s/N_0$ мало, разложение в (8.16) хорошо аппроксимируется с помощью лишь первого ненулевого члена. В этом случае обе формулы оценок, по существу, тождественны. Поэтому формула оценки, основанная на функции из (8.15), асимптотически оптимальна при $R\to 0$. Более того, как будет показано, та же самая формула оценки оптимальна также в другом крайнем случае, когда $R\to\infty$.

Анализ характеристик этих систем проводится так же, как соответствующий анализ системы отслеживания ФТ несущей. Дисперсия фазы в случае, когда ширина полосы шума эквивалентной системы ФАПЧ B_L мала по сравнению с $1/T_s$,

$$\sigma_\Phi^2 = 2\sigma_n^2 B_L T_s/A_e^2, \qquad (8.22)$$

где $\sigma_n^2 = -n^4\left[E\{c_l^n(\Phi) - [c_l^*(\Phi)]^n\}^2 - E^2\{c_l^n(\Phi) - [c_l^*(\Phi)]^n\}\right]$ — дисперсия сигнала на входе фильтра цепи и где A_l — эффективная амплитуда сигнала. После некоторых преобразований можно привести дисперсию шума $\sigma^2{}_n$ к виду

$$\sigma_n^2 = \frac{n^4}{2^{2n-3}} \sum_{k=1}^{n} \binom{n}{k}^2 k! \frac{1}{R^k} . \tag{8.23}$$

Из ф-лы (8.21) получаем также, что эффективная амплитуда сигнала

$$A_e = \frac{d}{d\Phi_e} \left\{ \frac{n^2}{2^{n-1}} \sin n\Phi_e \right\}_{\Phi_e=0} = \frac{n^3}{2^{n-1}} . \tag{8.24}$$

Таким образом,

$$\sigma_\Phi^2 = \frac{B_L T_s}{n^2} \sum_{k=1}^{n} \binom{n}{k}^2 k! \frac{1}{R^k} . \tag{8.25}$$

Когда R велико, получаем

$$\sigma_\Phi^2 \approx N_0 B_L / A^2. \tag{8.26}$$

Так как это выражение представляет собой дисперсию фазы в отсутствие какой-либо модуляции, то, очевидно, дисперсия представляет собой оптимальную характеристику, вообще достижимую на каком-либо устройстве отслеживания фазы несущей. Это подтверждает, что описанные системы асимптотически оптимальны при $R \to \infty$. Они также оптимальны, когда R мало (если и B_L достаточно мало), и в этом случае

$$\sigma_\Phi^2 \sim B_L T_s \frac{n!}{n^2} \frac{1}{R^n} . \tag{8.27}$$

Очевидно, что такие системы представляют практический интерес только для малых значений n, если R не является относительно большим.

8.4. Отслеживание фазы несущей при большом отношении сигнал/шум

Хотя только что рассмотренные системы отслеживания асимптотически оптимальны $R \to \infty$, существуют устройства, которые могут в некоторых случаях иметь лучшую характеристику, когда R велико, но конечно. Один из методов улучшения характеристик состоит в использовании аналога (7.4) как функции, на основании которой строится решение, т. е. в использовании функции

$$\max_j \exp \left\{ \frac{1}{N_0} \int_{lT_s}^{(l+1)T_s} [2y(t)\, x_j(t, \Phi) - x_j^2(t, \Phi)]\, dt \right\} . \tag{8.28}$$

Этот метод, который называется *обратной связью от решающего устройства,* заключается в определении вначале наиболее правдоподобного символа и последующей попытки оценить или уточнить оценку фазы несущей.

В качестве примера рассмотрим еще раз ФТ систему из предыдущего параграфа. Если R велико и j_l является значением j, максимизирующим (8.28), то

$$\frac{N_0}{2A}\,\frac{\partial \log_e p\,[y_l(t)\,|\,\Phi]}{\partial \Phi} \approx \int\limits_{lT_s}^{(l+1)\,T_s} y(t)\sqrt{2}\cos(\omega_c t+\theta_{j_l}+\Phi)\,dt. \qquad (8.29)$$

Это соотношение приводит к схеме устройства (рис. 8.4), которое отличается от обычной системы ФАПЧ лишь наличием фазовращателя, управляемого выходом приемника символов. Задержка на T_s секунд необходима в силу того, что нужно принять весь символ прежде, чем вынести решение относительно его фазы. Затем это решение используется для изменения выхода ГУН так, чтобы сформировать функцию, определяемую ф-лой (8.29). (Интегратор может быть исключен, так как он ни на что в действительности не влияет, если, как предполагалось, ширина полосы системы ФАПЧ B_L мала по сравнению с $1/T_s$.)

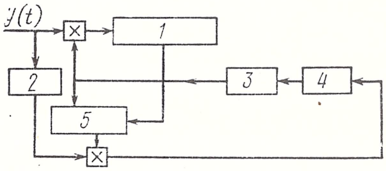


Рис. 8.4. Структурная схема синхронизатора ФТ несущей с обратной связью от решающего устройства:

1 — приемник символов; 2 — задержка на T_s, с; 3 — ГУН; 4 — фильтр ФАПЧ; 5 — фазовращатель

Если приемник символов всегда принимает правильное решение, то характеристика этого устройства совпадает с характеристикой системы ФАПЧ, имеющей тот же входной сигнал (но с немодулированной фазой) и имеющей тот же фильтр ФАПЧ. Влияние неправильного решения относительно символов состоит в снижении мощности сигнала на входе и в увеличении мощности шума. Предположим, что принимаемый сигнал имеет вид $y_l(t)=\sqrt{2}A\times$ $\times\sin(\omega_c t+\theta_r+\Phi_0)$ и что приемник выбирает фазы θ_s. Тогда обусловленная сигналом низкочастотная компонента на входе фильтра ФАПЧ в течение следующих T_s секунд будет равна

$$A\cos\theta_e\sin\Phi_e+A\sin\theta_e\cos\Phi_e, \qquad (8.30$$

где $\Phi_e=\Phi_0-\Phi$; Φ — текущая фаза ГУН и $\theta_e=\theta_r-\theta_s$. Первое слагаемое здесь является желаемым сигналом, амплитуда которого уменьшена в $\cos\theta_e$ раз; второе слагаемое характеризует шум. Легко показать, что этот шум будет некоррелирован с аддитивным шумом

$$n_1(t)=\sqrt{2}\,n(t)\cos(\omega_c t+\theta_s+\Phi). \qquad (8.31)$$

Рассматривая коррелятор с наибольшим выходом, отметим, что на этот выход в приемнике символов шум влияет лишь через посредство члена $\sqrt{2}n(t)\sin(\omega_c t+\theta_s+\Phi)$, который не зависит от $n_1(t)$. Выходы других корреляторов, конечно, не являются независимыми от $n_1(t)$, но вклад этих выходов, обусловленный $n_1(t)$, может с равной вероятностью принимать любой знак так, что результат не изменяется. Более того, некоррелированными также являются импульсы шума $A\sin\theta_e\cos\Phi_e$, соответствующие любым двум различным интервалам символов. Таким образом, когда $B_L \ll 1/T_s$, этот шум добавляет лишь коэффициент

$$\sigma^2 T_s \tag{8.32}$$

к низкочастотной спектральной плотности шума, где $\sigma^2 = A^2 E\{\sin^2\theta_e\cos^2\Phi_e\} \approx A^2 E\{\sin^2\theta_e\}$.

Так как средняя амплитуда сигнала уменьшается в $E(\cos\theta_e)$ раз, то дисперсия фазовой ошибки на выходе ГУН приближенно равна

$$\sigma_\Phi^2 = \frac{N_0 B_L}{A^2 E^2(\cos\theta_e)}\,[1 + RE(\sin^2\theta_e)]. \tag{8.33}$$

Самой распространенной ошибкой при больших отношениях сигнал/шум R является выбор фазы, ближайшей к правильной фазе. Таким образом, для n-фазовой ФТ $|\theta_e| = 2\pi/n$ с большой вероятностью и

$$E^2(\cos\theta_e) \approx \left[1 - \left(1 - \cos\frac{2\pi}{n}\right)P_e\right]^2;$$

$$E(\sin^2\theta_e) \approx \left(\sin^2\frac{2\pi}{n}\right)P_e, \tag{8.34}$$

где P_e — вероятность ошибки в символе.

Тот же метод применим так же, когда для модуляции используется ортогональная ЧТ или ВИМ. Фазовращатель на рис. 8.4 должен быть заменен устройством сдвига частоты или стробирующим устройством соответственно. Так как сигналы ортогональны, то при ошибочном решении относительно символа шум будет оставаться неизменным, а сигнал полностью устраняется. Таким образом, дисперсия фазовой ошибки такой системы

$$\sigma_\Phi^2 \approx N_0 B_L / A^2 (1 - P_e)^2, \tag{8.35}$$

где опять P_e — вероятность ошибки в символе. Это, конечно, предполагает наличие близкой к идеальной символьной синхронизации, позволяющей устранить символьную модуляцию до того, как сигнал поступит на вход фильтра ФАПЧ.

Одним из возможных недостатков описанного метода является требование задержки на T_s секунд. Если выход приемника символов можно использовать для получения оценки текущего наиболее вероятного принимаемого символа в каждый момент времени, то эту задержку можно вообще исключить. В случае двоичной ФТ, например, оценка максимального правдоподобия символа, принимаемого в любой момент времени t, описывается знаком выхода коррелятора в момент t, т. е. функцией

$$s(t) \triangleq \operatorname{sgn} \int\limits_{lT_s}^{t} y(t)\sqrt{2}\sin(\omega_c t+\Phi)\,dt;\quad lT_s<t<(l+1)\,T_s. \tag{8.36}$$

Таким образом, когда используемым типом модуляции является двоичная **ФТ**, задержку в устройстве, изображенном на рис. 8.4, можно устранить, а фазовращатель заменить на умножитель, имеющий в качестве одного входа выход ГУН, а в качестве другого входа — функцию $s(t)$.

Очевидно, что это модифицированное устройство будет хуже устройства, имеющего задержку, так как начальные оценки $s(t)$ будут неверными с вероятностью, близкой к 1/2. Дисперсия фазы в обоих случаях будет задаваться ф-лой (8.33) при $E(\sin^2\theta_e)=0$, $E^2(\cos\theta_e)=(1-2P_0)^2$. Для цепи с задержкой P_0 обозначает вероятность ошибки в символе. Для модифицированной цепи P_0 обозначает процент времени, когда $s(t)$ имеет неправильный знак, т. е.

$$P_0=\frac{1}{2}-\frac{1}{T_s}\,\frac{1}{\sqrt{2\pi}}\int\limits_0^{T_s}\int\limits_0^{[2R\,(t/T_s)]^{1/2}} e^{-x^2/2}\,dx\,dt=$$

$$=\frac{1}{2}-\frac{1}{\sqrt{2\pi}}\int\limits_0^{(2R)^{1/2}}\left(1-\frac{x^2}{2R}\right)e^{-x^2/2}\,dx=\frac{1}{2}-\frac{1}{2}\left(1-\frac{1}{2R}\right)\operatorname{erf}(R^{1/2})-$$

$$-\frac{1}{2\pi^{1/2}R^{1/2}}\,e^{-R}. \tag{8.37}$$

Следовательно,

$$(1-2P_0)^2=\left[\left(1-\frac{1}{2R}\right)\operatorname{erf}(R^{1/2})+\frac{1}{R^{1/2}\pi^{1/2}}\,e^{-R}\right]^2\approx$$

$$\approx\begin{cases}1, & R\gg 1;\\ \dfrac{16}{9\pi}R, & R\ll 1\end{cases} \tag{8.38}$$

и

$$\sigma_\Phi^2\approx B_L T_s\left\{\frac{1}{R\,(1-2P_0)^2}\right\}\approx\begin{cases}B_L T_s\dfrac{1}{R}, & R\gg 1;\\[2ex] \dfrac{9\pi}{16}\,B_L T_s\dfrac{1}{R^2}, & R\ll 1.\end{cases} \tag{8.39}$$

Для цепи отслеживания с задержкой при двоичной **ФТ** имеем

$$P_e=\frac{1}{2}-\frac{1}{\sqrt{2\pi}}\int\limits_0^{(2R)^{1/2}} e^{-x^2/2}\,dx=\frac{1}{2}\left(1-\operatorname{erf}R^{1/2}\right) \tag{8.40}$$

и

$$\sigma_\Phi^2\approx B_L T_s\left\{\frac{1}{R\,(1-2P_e)^2}\right\}\approx\begin{cases}B_L T_s\dfrac{1}{R}, & R\gg 1;\\[2ex] \dfrac{\pi}{4}\,B_L T_s\dfrac{1}{R^2}, & R\ll 1.\end{cases} \tag{8.41}$$

Оба эти выхода не учитывают эффекты второго порядка, которые в действительности приводят к более быстрому ухудшению характеристики системы при уменьшении отношения сигнал/шум R. При определении P_0 и P_e считалось, что опорная несущая точно известна. Однако при уменьшении R опорная фаза несущей будет становиться все менее и менее точной, приводя тем самым к уменьшению эффективного отношения сигнал/шум на входе и, следовательно, к дальнейшему увеличению P_e и P_0. Тем не менее, если σ_Φ^2 достаточно мала, то этот эффект будет фактически оставаться пренебрежимо малым, и приближенные выражения (8.39) и (8.41) будут давать близкие к истинным характеристики этих систем.

8.5. Система Костаса и квадратичная система

Все методы отслеживания фазы в предыдущих параграфах предполагали предварительное установление символьной синхронизации. Эта операция в действительности не столь существенна для характеристики системы отслеживания. В худшем случае, когда символьная синхронизация имеет ошибку в $T_s/2$ секунд, средняя амплитуда сигнала на входе фильтра системы уменьшается лишь в два раза, например, для ФТ и АИМ (когда распределение амплитуды символа симметрично относительно нуля). Поэтому дисперсия фазовой ошибки увеличивается самое большое в четыре раза при отсутствии символьной синхронизации.

В этом параграфе, однако, будет показано, что можно получить даже меньшее ухудшение характеристики, когда символьная синхронизация не осуществлена, если устройство отслеживания строится без предположения о наличии этой информации. Метод состоит просто в замене интеграторов в системе фильтрами нижних частот. Так как лишь для этих интеграторов требуется символьная синхронизация, то измененная система будет абсолютно независимой от этой информации. Хотя тот же подход может быть использован для всех систем из § 8.3, ниже ограничимся лишь системами для АИМ и двоичной ФТ.

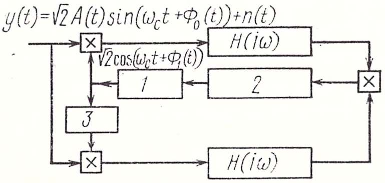

$y(t)=\sqrt{2}A(t)\sin(\omega_c t+\Phi_0(t))+n(t)$
$H(i\omega)$
$\sqrt{2}\cos(\omega_c t+\Phi_1(t))$
1
2
3
$H(i\omega)$

Рис. 8.5. Структурная схема цепи Костаса:

1 — ГУН; *2* — фильтр ФАПЧ; *3* — поворот фазы на 90°

Эти две системы идентичны и имеют вид, изображенный на рис. 8.5, когда интеграторы заменены произвольными фильтрами. Это устройство часто называется *системой Костаса*. Эта система может быть исследована методом, который во многих чертах совпадает с использованным для обычной системы ФАПЧ. Пусть принимаемый сигнал имеет вид $y(t)=\sqrt{2}A(t)\sin[\omega_c t+\Phi_0(t)]+n(t)$. Тогда сигнал на выходе верхнего фильтра (рис. 8.5) может быть записан в виде $A_1(t)\sin\Phi_e(t)+n_1(t)$, где $A_1(t)$ — результат фильтрации $A(t)$, $\Phi_e(t)=\Phi_0(t)-\Phi_1(t)$ и где $n_1(t)$ — профильтрованное произведение

$n(t)\sqrt{2}\cos[\omega_c t+\Phi_1(t)]$. Аналогично сигнал на выходе нижнего фильтра имеет вид $A_1(t)\cos\Phi_e(t)+n_2(t)$, где $n_2(t)$ — профильтрованное произведение $n(t)\sqrt{2}\sin[\omega_c t+\Phi_1(t)]$. Если эти фильтры широкополосны по отношению к ширине полосы системы B_L (и так как ширина полосы фильтров будет порядка $1/T_s$, это предположение совпадает со сделанным в предыдущем параграфе), то результаты § 5.5 применены здесь в равной мере. В частности, отождествляя $\sqrt{2}n_1(t)$ с $n'(t)$ из (5.53) и $\sqrt{2}n_1(t)$ с $n''(t)$ из того же самого равенства, получаем, что $n_1(t)$ и $n_2(t)$ — независимые совместно гауссовские процессы и с точки зрения остальной части цепи, по существу, белые. (То есть $E\{n_1(t)n_1(t+\tau)\}=E\{n_2(t)n_2(t+\tau)\}\approx 0$ для $\tau\gg 1/B_n$, где B_n обозначает ширину полосы шума каждого из фильтров.) Более того, так как $\Phi_e(t)$ — медленно меняющаяся функция времени (т. е. так как ширина полосы цепи мала), то $n_1(t_2)$, по существу, не зависит от $\Phi_e(t_1+\tau)$ и, следовательно, также от $A_1(t_1+\tau)$ при $t_1\leqslant t_2$ и $\tau\ll 1/B_L$ [и аналогично для $n_2(t_2)$; см. § 5.5]. Таким образом, находим, например, что

$$E\{n_1(t)\,n_1(t+\tau)\,A_1(t)\sin\Phi_e(t)\,A_1(t+\tau)\sin\Phi_e(t+\tau)\}\approx$$

$$\approx\begin{cases} E\{n_1(t)\,n_1(t+\tau)\}\,E\{A_1(t)\,A_1(t+\tau)\sin^2\Phi_2(t)\}, & \tau\ll 1/B_L;\\ E\{n_1(t)\,A_1(t)\sin\Phi_e(t)\,A_1(t+\tau)\sin\Phi_e(t+\tau)\}\,E[n_1(t+\tau)]=0, & \tau\gg 1/B_n \end{cases} \qquad (8.42)$$

и если $B_n\gg B_L$, то имеем

$$E\{n_1(t)\,n_1(t+\tau)\,A_1(t)\sin\Phi_e(t)\,A_1(t+\tau)\sin\Phi_e(t+\tau)\}\approx$$
$$\approx R_{n_1}(\tau)\,E\{A_1(t)\,A_1(t+\tau)\sin^2\Phi_e(t)\} \qquad (8.43)$$

для всех τ.

Используя (8.43) и аналогичные аппроксимации для других математических ожиданий того же самого вида, приходим к следующим выводам:

1) Сигнал $A_1^2(t)\sin\Phi_e(t)\cos\Phi_e(t)=\frac{1}{2}A_1^2(t)\sin 2\Phi_e(t)$ на выходе фильтра ФАПЧ не коррелирован с шумом $n'(t)=n_1(t)A_2(t)\times\cos\Phi_e(t)+n_2(t)A_2(t)\sin\Phi_e(t)+n_1(t)n_2(t)$ на этом входе.

2) Автокорреляционная функция шума $R_{n'}(\tau)$ может быть выражена в виде

$$R_{n'}(\tau)=R_{n_i}(\tau)\,R_{A_1}(\tau)+R^2_{n_i}(\tau), \qquad (8.44)$$

где $R_{n_i}(\tau)=R_{n_1}(\tau)=R_{n_2}(\tau)$ и, конечно, $R_{A_1}(\tau)=E\{A_1(t)A_1(t+\tau)\}$.

Наконец, опять-таки, из-за того, что $B_L\ll 1/T_s$, амплитуда сигнала на входе фильтра ФАПЧ может быть аппроксимирована средним значением, как в § 8.2. В соответствии с этим, если $\Phi_e(t)$ остается малой, система отслеживания (см. рис. 8.5) хорошо аппроксимируется обычной линейной моделью системы ФАПЧ (ср. с рис. 8.2), входом которой является функция $\Phi_0(t)+n'(t)/E[A_1^2(t)]$.

Поэтому дисперсия фазовой ошибки, обусловленной аддитивным шумом, приближенно равна

$$\sigma_\Phi^2 = \frac{2B_L\, S_{n'}(0)}{E^2\ [A_1^2(t)]}\,. \tag{8.45}$$

где B_L — ширина полосы шума линейной модели цепи; из (8.44) получаем

$$S_{n'}(0) = \int\limits_{-\infty}^{\infty} R_{n'}(\tau)\,d\tau = \int\limits_{-\infty}^{\infty} S_{A_1}(f)\,S_{n_i}(-f)\,df + \int\limits_{-\infty}^{\infty} S_{n_i}(f)\,S_{n_i}(-f)\,df. \tag{8.46}$$

Но

$$A_1(t) = \int\limits_{0}^{\infty} h(\tau)\,A(t-\tau)\,d\tau, \tag{8.47}$$

где $h(t)$ — импульсный отклик фильтров, стоящих перед умножителем. Следовательно, если $S_A(f)$ — спектральная плотность процесса $A(t)$, то

$$E\,[A_1^2(t)] = \int\limits_{-\infty}^{\infty} S_A(f)\,|H(\mathrm{i}\,2\pi f)|^2\,df. \tag{8.48}$$

Аналогично, когда $n(t)$ — белый шум с односторонней спектральной плотностью N_0, то

$$S_{n_i}(f) = \frac{N_0}{2}\,|H(\mathrm{i}\,2\pi f)|^2; \tag{8.49}$$

$$S_{n'}(0) = \frac{N_0}{2}\int\limits_{-\infty}^{\infty} S_A(f)|H(\mathrm{i}2\pi f)|^4\,df + \left(\frac{N_0}{2}\right)^2 \int\limits_{-\infty}^{\infty} |H(\mathrm{i}\,2\pi f)|^4\,df. \tag{8.50}$$

Таким образом,

$$\sigma_\Phi^2 = N_0 B_L \left\{ \frac{\int\limits_{-\infty}^{\infty} S_A(f)\,|H(\mathrm{i}\,2\pi f)|^4\,df + \frac{N_0}{2}\int\limits_{-\infty}^{\infty} |H(\mathrm{i}\,2\pi f)|^4\,df}{\left[\int\limits_{-\infty}^{\infty} S_A(f)|H(\mathrm{i}2\pi f)|^2\,df\right]^2} \right\}. \tag{8.51}$$

Считается, что оптимальный фильтр $H(\mathrm{i}\omega)$ — это фильтр, который минимизирует σ_Φ^2. Но минимизация σ_Φ^2 эквивалентна минимизации числителя в (8.51) при условии, что знаменатель остается постоянным или, что более удобно, остается постоянным корень квадратный из знаменателя. Таким образом, требуется найти частотную характеристику $H(\mathrm{i}\omega)$, которая минимизирует выражение

$$\int_{-\infty}^{\infty}\{[S_A(f)+N_0/2]\,|H(\mathrm{i}\,2\pi f)|^4-\lambda S_A(f)\,|H(\mathrm{i}\,2\pi f)|^2\}\,df=$$

$$=\int_{-\infty}^{\infty}\left\{[S_A(f)+N_0/2]\left[|H(\mathrm{i}\,2\pi f)|^2-\frac{\lambda S_A(f)}{2[S_A(f)+(N_0/2)]}\right]^2-\right.$$

$$\left.-\frac{\lambda^2 S_A^2(f)}{4[S_A(f)+(N_0/2)]}\right\}df. \tag{8.52}$$

Этот интеграл, очевидно, достигает своего минимального значения, когда

$$|H(\mathrm{i}\,2\pi f)|^2=\frac{(\lambda/2)\,S_A(f)}{S_A(f)+(N_0/2)}\,. \tag{8.53}$$

Это и есть частотная характеристика оптимального фильтра. Так как (8.53) является условием, относящимся лишь к $|H(\mathrm{i}\omega)|^2$, то $H(\mathrm{i}\omega)$ может, очевидно, описывать физически реализуемый фильтр. Постоянная $\lambda/2$ произвольна, так как она не влияет на отношение (8.51). Когда $H(\mathrm{i}\omega)$ определяется согласно (8.53), это отношение будет равно

$$\sigma_\Phi^2=\frac{N_0B_L}{\displaystyle\int_{-\infty}^{\infty}\frac{S_A^2(f)}{S_A(f)+(N_0/2)}\,df}\,. \tag{8.54}$$

Для АИМ или двоичной ФТ с прямоугольными импульсами спектр процесса $A(t)$ имеет вид

$$S_A(f)=P_sT_s\left(\frac{\sin\pi fT_s}{\pi fT_s}\right)^2, \tag{8.55}$$

где P_s — средняя мощность принимаемого сигнала. Хотя общее выражение для σ_Φ^2 довольно громоздко, если спектр $S_A(f)$ задается равенством (8.55), легко найти его асимптотические выражения при больших и малых отношениях сигнал/шум. Если $N_0/2\ll S_A(f)$ (для всех f, для которых вклад $S_A(f)$ в общую энергию сигнала является существенным), то

$$\sigma_\Phi^2\approx N_0B_L/P_s=B_LT_s/R, \tag{8.56}$$

где $R=P_sT_s/N_0$. Это выражение (между прочим, не зависящее от спектра сигнала) описывает дисперсию фазы, которая имела бы место в отсутствие какой-либо модуляции. В другом крайнем случае, когда $N_0/2\gg S_A(f)$ для всех f, имеем

$$\sigma_\Phi^2\approx\frac{N_0^2B_L}{2\displaystyle\int_{-\infty}^{\infty}S_A^2(f)\,df}=\frac{3N_0^2B_L}{4P_s^2T_s}=\frac{3}{4}\,\frac{B_LT_s}{R^2}\,. \tag{8.57}$$

Дисперсия фазовой ошибки, которая получается при использовании систем предыдущего параграфа для АИМ и двоичной ФТ, как было показано, равна

$$\sigma^2_{\Phi} = B_L T_s (1/R + 1/2R^2). \tag{8.58}$$

Таким образом, когда R велико, характеристики в этих двух случаях почти совпадают; когда R мало, дисперсия системы Костаса больше в 3/2 раза. В качестве последнего сравнения оценим чувствительность системы к неоптимальному выбору фильтра $H(\mathrm{i}\omega)$; предположим, что выбрали

$$H(\mathrm{i}\, 2\pi f) = \begin{cases} 1, & |f| < \dfrac{1}{T_s}; \\ 0, & |f| > \dfrac{1}{T_s}. \end{cases} \tag{8.59}$$

Тогда, так как $P_s T_s \int\limits_{-1/T_s}^{1/T_s} \left(\dfrac{\sin \pi f T_s}{\pi f T_s}\right)^2 df \approx P_s$, то

$$\sigma^2_{\Phi} \approx \frac{B_L N_0 (P_s + N_0/T_s)}{P_s^2} = B_L T_s \left(\frac{1}{R} + \frac{1}{R^2}\right). \tag{8.60}$$

Можно получить интересное видоизменение этого метода Костаса для отслеживания фазы. Пусть $y(t)$ будет входом системы Костаса и пусть $h(t)$ обозначает импульсный отклик каждого из двух фильтров, стоящих перед умножителями. Тогда выход верхнего фильтра

$$\int\limits_{-\infty}^{\infty} y(\tau) \sqrt{2} \cos [\omega_c \tau + \Phi_1(\tau)]\, h(t - \tau)\, d\tau. \tag{8.61}$$

Но так как этот фильтр, по предположению, считается широкополосным относительно ширины полосы системы, то $\Phi_1(\tau) \approx \Phi(t)$ для всех τ, для которых значения $h(t-\tau)$ не являются пренебрежимо малыми. Таким образом, выход верхнего фильтра может быть записан в виде

$$\left(\int\limits_{-\infty}^{\infty} y(\tau) \cos \omega_c \tau\, h(t - \tau)\, d\tau\right) \sqrt{2} \cos [\Phi_1(t)] - \left(\int\limits_{-\infty}^{\infty} y(\tau) \sin \omega_c \tau\, h(t - \tau)\, d\tau\right) \sqrt{2} \sin [\Phi_1(t)] \triangleq Y(t) \sqrt{2} \cos \Phi_1(t) - X(t) \sqrt{2} \sin \Phi_1(t). \tag{8.62}$$

Аналогично выход нижнего фильтра равен

$$Y(t) \sqrt{2} \sin \Phi_1(t) + X(t) \sqrt{2} \cos \Phi_1(t), \tag{8.63}$$

так что входом фильтра ФАПЧ будет

$$[Y^2(t) - X^2(t)] \sin 2\Phi_1(t) + 2X(t)\,Y(t) \cos 2\Phi_1(t). \tag{8.64}$$

Рассмотрим теперь в момент t квадрат выхода фильтра, имеющего импульсный отклик $h(t)\cos\omega_c t$:

$$\left(\int_{-\infty}^{\infty} y(\tau)\, h(t-\tau) \cos[\omega_c (t-\tau)]\, d\tau\right)^2 = \frac{1}{2}[X^2(t) + Y^2(t)] +$$

$$+ \frac{1}{2}[Y^2(t) - X^2(t)] \cos 2\omega_c t + X(t)\,Y(t) \sin 2\omega_c t. \tag{8.65}$$

Если этот сигнал умножить на $4\sin 2[\omega_c t + \Phi_1(t)]$, то полученное низкочастотное слагаемое будет задаваться соотношением (8.64).

Таким образом, другой реализацией системы Костаса, называемой *квадратичной цепью,* является та, которая изображена на рис. 8.6. Так как сигналы ошибок в обеих цепях одни и те же, то они дают одинаковые опорные несущие. Выбор между этими двумя устройствами производится исключительно с точки зрения простоты реализации, которая, в свою очередь, зависит от частот и ширины полос рассматриваемых устройств. То же справедливо, когда $h(t)$ является характеристикой согласованного фильтра, при этом $h(t)\cos\omega_c(t)$ будет представлять некогерентный согласованный фильтр. Поэтому оптимальные системы отслеживания несущей для АИМ и двоичной ФТ из § 8.2 и 8.3 также могут быть реализованы как квадратичные системы. Наконец, очевидным обобщением этого рассуждения можно показать, что система отслеживания несущей для n-ичной ФТ из § 8.3 эквивалентна *системе n-й степени.* В последней за фазовонекогерентным согласованным фильтром включается устройство, возводящее в n-ю степень, а его выход отслеживается обычной системой ФАПЧ (с умножителем частоты в n раз, включенным после ГУН).

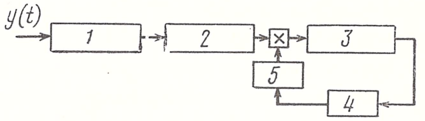


Рис. 8.6. Структурная схема квадратичной цепи:

1 — полосовой фильтр; *2* — квадратичное устройство; *3* — фильтр ФАПЧ; *4* — ГУН; *5* — умножитель на 2

8.6. Отслеживание символов, имеющих «тонкую структуру»

Принципиальное отличие дисперсий ошибок отслеживания в цепях отслеживания символов, описанных в гл. 7, от дисперсий в системах отслеживания несущей, рассматриваемых в этой главе, состоит в том, что последние относительно независимы от символьных статистик. Эта независимость возникала из-за того, что частота несущей предполагалась большой по сравнению с обратной величиной периода символа. Таким образом, каждый символ состоял из многих периодов несущей, и корреляция между местной опорной несущей и принимаемой несущей, вообще говоря, не зависела от относительно редких переходов символов. Системы отслеживания символов в противоположность этому использовали частично (или полностью, как в случае прямоугольных импульсов) наличие переходов символов при формировании сигнала ошибки.

Если не использовать переходы символов, то преимущества очевидны, в особенности, когда последовательные символы не являются статистически независимыми. Для реализации этого преимущества следует придать символам «тонкую структуру», подобную той, которую имеет несущая. В частности, можно допустить, что ν-й символ имеет вид $x_\nu(t)\sigma(t)$, где $x_\nu(t)$ определяется так же, как в гл. 3 и 4, и зависит от вида модуляции, а $\sigma(t)$ задает тонкую структуру. Здесь мы будем предполагать, что сигнал $\sigma(t)$ имеет период T_s, равный периоду символа. Если бы период $\sigma(t)$ был меньше, чем T_s, то тонкая структура могла бы быть отслежена без помощи однозначно устанавливаемой символьной синхронизации, и введение этой структуры потеряло бы во многом свой смысл.

Системы отслеживания, рассмотренные в § 7.6, в равной мере можно использовать и тогда, когда символы имеют вид $x_\nu(t)\sigma(t)$. Согласованные фильтры, конечно, должны теперь быть согласованы с этими измененными символами. Один из методов реализации этой модификации иллюстрируется рис. 8.7*а* для когерентной АИМ и двоичной ФТ и рис. 8.7*б* для некогерентной АИМ и недвоичной ФТ. Так как сигнал умножается на $\sigma(t)$ до того, как он проходит через блоки, названные «согласованным фильтром», то эти фильтры согласованы с импульсом, который наблюдался бы в отсутствие тонкой структуры.

Здесь также можно использовать методы анализа характеристик систем, развитые в § 7.6. Дисперсия (в радианах в квадрате) ошибки отслеживания

$$\sigma_\Phi^2 \approx \frac{2S_n(0)\,B_L}{A_e^2}, \tag{8.66}$$

где $A_e = \frac{1}{2\pi}\left|\frac{\partial}{\partial\tau} E\left\{\zeta\left(\tau+\frac{\Delta t}{2}\right)-\zeta\left(\tau-\frac{\Delta t}{2}\right)\right\}\right|_{\tau=0}$ и $S_n(0) = \frac{\Delta^2(\Delta t, -\Delta t/2)}{T_s}$ при $\Delta^2(u, t) = \lim\limits_{M\to\infty}\frac{1}{M}\operatorname{var}[\zeta(t)-\zeta(t+u)]$ [ср. с равенствами (7.74) и (7.84)]. Функция $\zeta(t)$ обозначает (нормированный) выход квадратичного устройства системы (рис. 8.7) в момент t.

Так как цель введения тонкой структуры — сделать сигнал ошибки, по существу, независимым от символьных статистик, то можно предположить, что функция $\sigma(t)$ такова, что эта цель достигнута. В соответствии с этим среднее и дисперсия случайной величины $\zeta(t)$ определяются так же, как в § 6.6 [равенства (6.74), (6.75) при $\zeta_\nu=\zeta(t=\nu\Delta T)$], и являются функциями лишь отношения сигнал/шум и автокорреляционной функции $\rho(\tau)$ процесса $\sigma(t)$.

Чтобы преобразовать равенство (8.66) к более удобному виду, предположим, что $\sigma(t)$ является псевдошумовой последовательностью с периодом T_s и с длительностью бита $\Delta t = T_s/n$. Тогда

$$\rho(\tau)=\int_0^{T_s}\sigma(t)\,\sigma(t+\tau)\,dt=\begin{cases}1-\dfrac{n+1}{n}\,\dfrac{\tau}{\Delta t}, & |\tau|<\Delta t;\\[2ex] -\dfrac{1}{n}, & |\tau|\geqslant\Delta t\,(\mathrm{mod}\,T_s)\end{cases}\qquad(8.67)$$

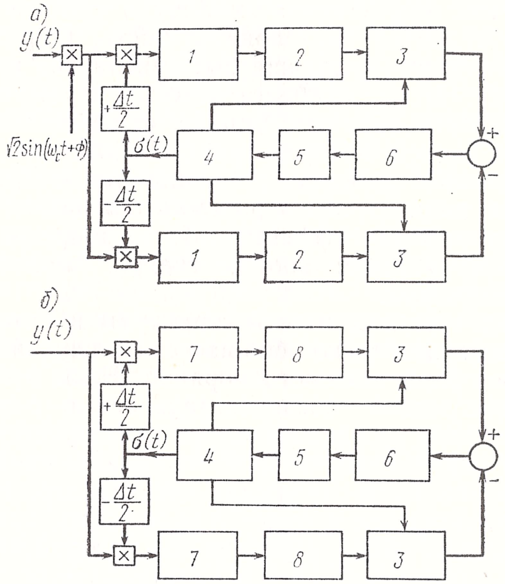


Рис. 8.7. Структурные схемы устройств отслеживания символов, имеющих тонкую структуру:

а) когерентный случай; *б*) некогерентный случай

1 — согласованный фильтр; *2* — квадратичное устройство; *3* — выборка и запоминание; *4* — генератор сигнала; *5* — ГУН; *6* — фильтр ФАПЧ; *7* — некогерентный согласованный фильтр; *8* — квадратичный детектор огибающей

и для больших n имеем

$$\sigma_\Phi^2 = 2\pi^2\left(\frac{\Delta t}{T_s}\right)^2\left(\frac{1}{R}+\frac{c_0}{R^2}\right)B_L T_s,\qquad(8.68)$$

где

$$R=\begin{cases}A^2E(x^2)\,T_s/N_0 & \text{для АИМ [ср. с (8.12)];}\\ A^2T_s/N_0 & \text{для ФТ;}\end{cases}$$

$$c_0=\begin{cases}1 & \text{для когерентной АИМ и двоичной ФТ;}\\ 2 & \text{для некогерентной АИМ и недвоичной ФТ.}\end{cases}$$

Эта дисперсия выражена в радианах в квадрате (2π рад соответствуют T_s секундам).

Заметим, что корень квадратный из среднеквадратической ошибки отслеживания не только не зависит от символьных статистик [исключение составляет член $E(x^2)$ в случае АИМ], но и пропорционален множителю $(\Delta t/T_s)$. Это очевидное преимущество использования длинной последовательности полностью сводится, однако, на нет тем, что допустимая ошибка отслеживания уменьшается в то же число раз из-за наличия последовательности. Более того, так как эффективная амплитуда сигнала A_e увеличивается, когда добавляется последовательность, ширина полосы цепи B_L также, по-видимому, должна быть увеличена из-за ее присутствия (см. § 6.3). Часто наиболее важным ограничением на длину последовательности является, однако, ограничение на ширину полосы; ширина полосы, которая требуется для того, чтобы вместить модифицированные символы, увеличивается в $T_s/\Delta t$ раз. Так как это отношение должно быть разумно большим для того, чтобы тонкая структура была эффективной, то вопросы расширения полосы при этом подходе, вообще говоря, приводят к наиболее серьезным проблемам.

Этот метод введения тонкой структуры в поток символов для целей синхронизации легко обобщается на случай, когда требуется синхронизация более высокого порядка. Если $\sigma(t)$, например, является псевдошумовой последовательностью с периодом kT_s, то отслеживание этой последовательности в приемнике приводит к определению одной единственной точки в каждой последовательности k символов. Если отношение $T_s/\Delta t$ поддерживается большим, то ошибка отслеживания будет по-прежнему приближенно задаваться равенством (8.68). Причина, по которой этот результат является лишь приближенным в рассматриваемом случае, состоит в том, что теперь фильтры, стоящие перед квадратичными устройствами, согласованы только с отрезками полной псевдошумовой последовательности. Таким образом, сигнал ошибки определяется не автокорреляционной функцией (8.67) (в силу того, что T_s больше не является периодом ПШ последовательности), а множеством функций

$$\rho_i(\tau) = \int_{iT_s}^{(i+1)\,T_s} \sigma(t)\,\sigma(t+\tau)\,dt. \tag{8.69}$$

Однако эти *функции частичной автокорреляции* описываются все еще приближенно выражением (8.67) (с соответствующей нормировкой), *если* Δt достаточно мало по сравнению с T_s.

Так как дисперсия фазовой ошибки (8.68) не зависит от символьной модуляции, то это выражение должно быть справедливым даже в отсутствие какой-либо модуляции. Поэтому оно представляет собой также фазовую ошибку при отслеживании некогерентной псевдошумовой последовательности или, что эквивалентно, последовательности прямоугольных импульсов длительности Δt (ср.

с § 6.6). В последнем случае устройство, производящее выборки в схеме рис. 8.7*б*, может все же потребоваться, например, если фаза несущей, будучи относительно постоянной на любом Δt-секундном интервале, не остается постоянной в течение T_s секунд. Однако, если фаза несущей, по существу, постоянна на любом T_s-секундном интервале (это предположение неявно подразумевается, если $\sigma(t)$ не равно нулю на всем интервале T_s секунд и если принимаемые символы не модулированы никаким другим сигналом), то устройство, производящее выборки (рис. 8.7*б*), очевидно, не является необходимым; выход детектора огибающей представляет собой нужный вход для цепи отслеживания в любой момент времени. Отсутствие устройства, производящего выборки, не изменило бы характеристику отслеживания, если бы не нелинейный элемент, стоящий перед ним. Наличие этой нелинейности может улучшить характеристику системы, если нет символьной модуляции, при устранении устройства, производящего выборки.

Анализ устройства, изображенного на рис. 8.7*б*, в случае, когда исключается устройство, производящее выборки, и когда согласованный фильтр заменяется на произвольный, проще анализа системы Костаса из § 8.5. Производя операции, аналогичные описанным в этом параграфе, можно проверить, что если $\sigma(t)$ является псевдошумовой последовательностью с периодом бита Δt, дисперсия фазовой ошибки на выходе этой модифицированной цепи отслеживания (когда отношение полос до цепи и цепи велико)

$$\sigma_\Phi^2 = 2\pi^2 \left(\frac{\Delta t}{T_s}\right)^2 \left\{\frac{1}{R} + \frac{2}{R^2}\,\frac{T_s}{2\pi}\int\limits_{-\infty}^{\infty} |H(\mathrm{i}\,\omega)|^4\, d\,\omega\right\} B_L\, T_s. \qquad (8.70)$$

Здесь $H(\mathrm{i}\omega)$ — преобразование Фурье $h(t)$, а $h(t)\cos\omega_c t$ представляет собой импульсный отклик фильтра, предшествующего квадратичному устройству. Если $h(t)$ — прямоугольный фильтр с полосой $B=1/2T_s$, то дисперсия фазовой ошибки здесь, по-видимому, совпадет с полученной при использовании согласованного фильтра, за которым включено устройство, производящее выборки. Если $h(t)$ представляет собой фильтр, согласованный с прямоугольным импульсом длительности T_s, то, устранив устройство, производящее выборки, получим в действительности небольшое улучшение.

Это утверждение, казалось бы, находится в противоречии с результатами § 6.6 относительно оптимального фазовонекогерентного синхронизатора. Однако противоречие возникает с моделью фазовой статистики, приводящей к указанным результатам, а не с самими результатами. А именно, включение устройства, производящего выборки, является следствием того условия, что фаза несущей $\Phi(t)$ постоянна на каждом интервале $iT_s<t<(i+1)T_s$, но не на интервале $iT_s+\tau<t<(i+1)T_s+\tau$ для любого $\tau\neq 0$ по модулю T_s. Как было указано ранее, эта модель в некотором отношении является идеализированной.

8.7. Заключительные замечания

Самым прямым методом получения необходимой для системы связи синхронизации является использование трех (или более) отдельных каналов: одного для передачи отсчетов времени (и несущей или поднесущей), одного для синхронизации более высокого порядка и одного для самой информации. У этого подхода имеются два недостатка. Первый состоит в том, что эти три канала должны быть каким-то образом уплотнены, чаще всего по времени или по частоте. Это не только увеличивает сложность системы, но часто приводит к межканальной интерференции, которая может ухудшить характеристику системы. Второй состоит в том, что мощность, предназначенная каналам синхронизации, представляет собой мощность, которая могла бы быть использована для передачи данных, если бы имелась возможность установить синхронизацию каким-либо другим образом.

В соответствии с этим в последних двух главах были исследованы методы, позволяющие устранить необходимость использования одного или обоих вспомогательных каналов. В гл. 7 были описаны и изучены процедуры, дававшие возможность произвести символьную синхронизацию непосредственно по последовательности принимаемых символов, что позволяет устранить, по крайней мере, частично необходимость использования одного из каналов синхронизации. (Методы установления синхронизации более высокого порядка, использующие поток данных, исследуются в последующих главах; см. также § 8.6.) Настоящая глава продолжила это направление, в ней рассматривались методы выделения отсчетов времени непосредственно из модулированной несущей.

Не должно удивлять то, что во всех случаях точность, с которой синхроинформация могла быть определена непосредственно из модулированного сигнала, была меньше, чем в случае использования отдельных каналов, когда оба канала имеют одну и ту же мощность сигнала. На самом деле, вероятно, следовало ожидать более ярко выраженного различия между этими двумя ситуациями. Но так как доля мощности, выделенная каналу синхронизации, по возможности должна быть малой, предпочтение может быть отдано синхронизационным оценкам, получаемым непосредственно из модулированного сигнала. Однако, чтобы подтвердить эту гипотезу, нужно найти оптимальное распределение мощности между информационным каналом и каналами синхронизации. Это одна из проблем, исследованных в гл. 9.

Задачи

8.1. Получить результат (7.96), используя метод, приведенный в § 8.2.

8.2. Показать, что система отслеживания для n-ичной ФТ из § 8.3 эквивалентна в условиях, которые были введены в § 8.5 при рассмотрении квадратичной системы, системе n-й степени, т. е. системе ФАПЧ, которой предшествуют полосовой фильтр и устройство, возводящее в n-ю степень.

8.3. Рассмотреть систему отслеживания несущей из предыдущей задачи для четырехфазной ФТ, заменив согласованные фильтры прямоугольными полосовыми фильтрами с шириной полосы $2/T_s$. Показать, что в этом случае дисперсия ошибки отслеживания приближенно равна

$$\sigma_\Phi^2 = (1/R + 36/R^2 + 18/R^3 + 8/R^4)\, B_L T_s.$$

Сравнить этот результат с соответствующим результатом, относящимся к случаю, когда используются согласованные фильтры.

8.4. Решить задачу 5.6, если $y(t)$ — искаженный шумом сигнал, двоичной ФТ $y(t) = \sqrt{2} A \sin(\omega_c t + \theta_l) + n(t)$, $lT_s < t < (l+1) T_s$, $\theta_l = 0$ или π, если устройство, возводящее в нечетную степень ν, заменяется устройством, возводящим в четную степень $\nu (x(t) \to |x(t)|^\nu)$, и если B_2 центрирована относительно $2\omega_c$. Показать, в частности, что в условиях, указанных в задаче 5.6, отношение сигнал/шум на выходе теперь обратно пропорционально $l + (\nu/2)^2$, но точность, с которой несущая может быть восстановлена по этому выходному сигналу, опять-таки не зависит от ν.

8.5. С помощью ф-лы (8.13) показать, что идеальная система отслеживания несущей для двоичной ФТ будет такой, как изображена на рис. 8.3*а*, но верхняя цепь будет содержать нелинейность вида $\mathrm{th}[2R(\cdot)]$. Сравнить эту систему с системами, которые обсуждались в § 8.3 и 8.4. В частности, показать, что, когда $R \to \infty$, эта система совпадает с системой, рассмотренной в § 8.4, но имеющей задержку.

8.6. Дисперсия всех систем отслеживания несущей, рассмотренных в этой главе, стремится к $B_L T_s / R$ при возрастании отношения сигнал/шум R. Та же самая дисперсия наблюдалась бы, если бы несущая была немодулированной, а синхронизатор представлял бы собой обычную систему ФАПЧ. Будет ли ширина полосы цепи B_L одной и той же в этих двух случаях? Будет ли одной и той же вероятность потери синхронизации?

Глава 9

ЗАДАЧА РАСПРЕДЕЛЕНИЯ МОЩНОСТИ

9.1. Введение

Каков бы ни был метод, использованный для установления требуемой синхронизации, эта синхронизация всегда будет несовершенной. Очевидно, что эта неточность будет приводить к некоторому ухудшению характеристики системы. Одной из задач главы является оценка этого эффекта. Знание такой оценки необходимо при вынесении суждения о всей системе связи в целом и для ответа, среди прочего, на вопрос о том, является ли предлагаемый метод синхронизации удовлетворительным для рассматриваемой ситуации. Эта информация, кроме того, даст возможность сказать, выгодно ли затратить бо́льшую мощность для целей синхронизации или система уже фактически «пересинхронизирована» в том смысле, что некоторая мощность, используемая для синхронизации, могла бы быть более эффективно использована для передачи информации. Вопрос о распределении мощности между синхронизационным и информационными сигналами также исследуется в этой главе.

Если известны статистические свойства ошибок в опорных сигналах, то, в принципе, легко определить их влияние на характеристику системы. Когда, например, мерой характеристики системы является отношение сигнал/шум на выходе и когда ошибки в синхронизации несущей, поднесущей¹⁾ и символов равны соответственно Φ_1, Φ_2 и Φ_3, необходимо вначале рассмотреть результирующее отношение сигнал/шум на выходе как функцию этих ошибок, т. е. $(S/N)=f(\Phi_1, \Phi_2, \Phi_3)$. Зная его, можно определить усредненную характеристику системы

$$(S/N)_{\text{AVE}} = \iiint t(\Phi_1, \Phi_2, \Phi_3)\, p\,(\Phi_1, \Phi_2, \Phi_3)\, d\Phi_1\, d\Phi_2\, d\Phi_3, \tag{9.1}$$

где $p(\Phi_1, \Phi_2, \Phi_3)$ — совместная плотность распределения ошибок трех опорных сигналов.

---

¹⁾ В предыдущих главах не делалось явного различия между несущими и поднесущими. Рассмотренные методы синхронизации были, в рамках использованных ограничений, одинаково применимы к случаям, когда используется одна или большее число несущих. (В когерентной системе с многими несущими, конечно, нужно предложить какой-нибудь метод получения опорных сигналов для всех несущих.) Однако неточное знание каждого из опорных сигналов приводит к ухудшению характеристики системы и поэтому должно быть принято во внимание при ее вычислении. Даже в этом случае обычно одна из несущих будет иметь наибольшее значение для рассматриваемой характеристики. Поэтому, а также и потому, что все равно нельзя рассмотреть все непредвиденные обстоятельства, бо́льшая часть последующего рассмотрения ограничена случаем, когда имеется одна единственная несущая. *(Прим. авт.)*.

Аналогично в дискретных системах, в которых имеет смысл вероятность ошибки, эта вероятность может быть вычислена как функция ошибок отсчетов времени и проинтегрирована по этим ошибкам для определения средней вероятности ошибки

$$P_e = \iiint P_e(\Phi_1, \Phi_2, \Phi_3)\, p(\Phi_1, \Phi_2, \Phi_3)\, d\Phi_1\, d\Phi_2\, d\Phi_3. \tag{9.2}$$

Функция $P_e(\Phi_1, \Phi_2, \Phi_3)$ обозначает вероятность ошибки при условии, что заданы ошибки опорных сигналов Φ_1, Φ_2 и Φ_3. Важно заметить, что соотношение (9.2) справедливо в случае, когда рассматриваются ошибки несущей и поднесущей, только если эти ошибки остаются относительно постоянными на интервале символа. В противном случае вероятность ошибки в символе зависит от всех прошлых ошибок опорного сигнала на символьном интервале.

Оба эти параметра, среднее отношение сигнал/шум и средняя вероятность ошибки, зависят от *плотности распределения* $p(\Phi_1, \Phi_2, \Phi_3)$ фазовых ошибок. Главное внимание в трех предыдущих главах было обращено на отыскание дисперсий этих ошибок при использовании различных оценивающих схем. К счастью, с хорошим приближением фазовые ошибки являются гауссовскими почти во всех случаях, представляющих практический интерес, и это свойство не зависит от процедуры оценивания. Более того, различные фазовые ошибки неизменно являются либо статистически независимыми (если они получаются из различных сигналов), либо прямо пропорциональными друг другу (если они получаются из одного и того же сигнала). Таким образом, представляют интерес лишь одномерные плотности распределения $p(\Phi_i)$, а если Φ_i — гауссовские случайные величины, то эти плотности полностью задаются с помощью дисперсий величин Φ_i. [Вообще говоря, $E(\Phi_i)$ будет равно нулю. Если, как рассматривалось в гл. 6 и 7, осуществляется *прием* метки символа и строится проверка гипотез, а не отслеживание, то ошибочное решение, конечно, будет приводить к постоянной ненулевой ошибке.]

Для того чтобы обосновать утверждение о том, что фазовые ошибки имеют приближенно гауссовское распределение, заметим вначале, что оно, очевидно, справедливо, когда оценка фазы является линейной функцией гауссовского шума, наложенного на сигнал. Таким образом, гауссовское приближение справедливо, когда оценка производится на выходе системы ФАПЧ при условии, что дисперсия фазовой ошибки достаточно мала (меньше, чем 1/4 рад^2 в случае синусоидальных сигналов; см. § 5.5). В большинстве представляющих для нас интерес ситуаций дисперсия фазовой ошибки в действительности достаточно мала для того, чтобы оправдать это предположение; если это не так, то, прежде всего, вероятность потери синхронизации будет неприемлемо большой.

Дополнительное обоснование справедливости предположения о гауссовском распределении фазовой ошибки требуется при рассмотрении системы отслеживания, которая содержит (или перед которой содержатся) и нелинейные элементы (гл. 7 и 8). Из-за нелинейностей шум на входе фильтра цепи перестает быть гауссовским, как предполагалось в § 5.5. Тем не менее, если ширина полосы системы много меньше ширины полосы фильтров, стоящих перед нелинейными устройствами (это предполагалось обычно в рассмотрениях гл. 7 и 8), то фазовая ошибка, относящаяся к любому моменту, представляет собой взвешенное среднее большого числа по существу независимых шумовых слагаемых. Поэтому, чтобы доказать, что даже в этом случае фазовая ошибка будет иметь приближенно гауссовское распределение, может быть применена центральная предельная теорема.

В последующем рассмотрении синхронизационный и информационный каналы будут считаться независимыми, и мы будем пренебрегать любым влиянием сигнала и шума одного канала на другие каналы. В некоторых случаях это предположение легко оправдать, как, например, тогда, когда оба канала достаточно разнесены друг от друга по частоте. Однако часто оно справедливо лишь при дополнительных ограничениях. Если, например, синхронизация устанавливается непосредственно по модулирующему сигналу, как было в последних двух главах, или если синхронизационный и информационный каналы пересекаются по спектру, то шумы на выходах этих двух каналов могут не быть независимыми. Эти шумы, однако, становятся, по существу, независимыми, если они рассматриваются на выходах фильтров с сильно отличающимися ширинами полос. В этом случае шум на выходе узкополосного фильтра составляет пренебрежимо малую часть выхода широкополосного фильтра, и, следовательно, он почти не коррелирован с ним. Так как ширина полосы демодулятора, вообще говоря, имеет порядок $1/T_s$, то это условие удовлетворяется, если ширина полосы шума синхронизатора B_L мала по сравнению с $1/T_s$ ¹⁾. Это ограничение, напомним, постоянно возникало из других соображений при рассмотрении синхронизаторов в предыдущих двух главах. Даже тогда, когда шумы в этих двух каналах могут считаться независимыми, может происходить взаимная интерференция сигналов. В дальнейшем будем ею пренебрегать. Однако следует сделать предостережение о том, что в некоторых случаях интерференцию нужно принимать во внимание для того, чтобы имел смысл анализ характеристики системы [ср. с задачей (9.3)].

Следует указать, что среднее отношение сигнал/шум и средняя вероятность ошибки являются в некотором смысле произвольными мерами. В некоторых случаях лучшей мерой, например, может быть доля времени, в течение которого вероятность ошибки превышает определенное значение или отношение сигнал/шум находится ниже некоторого заранее заданного уровня. Тем не менее, в силу того, что среднее этих величин является наиболее часто используемой мерой, рассмотрения последующих параграфов свя-

---

¹⁾ Это также справедливо при довольно нереальном противоположном условии $B_L \gg 1/T_s$. *(Прим. авт.)*.

заны лишь со средним отношением сигнал/шум или средней вероятностью ошибки независимо от нужд приложений. В случае необходимости можно легко обобщить этот подход на другие меры.

9.2. Влияние неточностей в опорных сигналах. Амплитудно-импульсная модуляция

Рассмотрим вначале влияние фазовой ошибки несущей (или поднесущей) на наблюдаемое отношение сигнал/шум в АИМ системе. Если принимаемый сигнал имеет вид

$$y(t)=\sqrt{2}\,Ax\sin\omega_c t+n(t) \tag{9.3}$$

и местной оценкой несущей является $\sqrt{2}\sin(\omega_c t-\Phi)$, то приемник, рассмотренный в гл. 3, вычисляет интеграл

$$I=\frac{1}{AT_s}\int\limits_0^{T_s} y(t)\sqrt{2}\sin(\omega_c t-\Phi)\,dt. \tag{9.4}$$

Так же, как и в гл. 3, определим отношение сигнал/шум на выходе как отношение дисперсии сигнала к среднеквадратической ошибке оценивания. В соответствии с этим для любого заданного Φ имеем

$$\left(\frac{S}{N}\right)_\Phi=\frac{\operatorname{var}(x)}{E\,(I-x)^2}=\frac{2R}{1+2R'\,(1-\cos\Phi)^2}\,, \tag{9.5}$$

где $R=(A^2T_s/N_0)\operatorname{var}(x)$ и $R'=(A^2T_s/N_0)E(x^2)$.

Если ошибка фазы опорной несущей имеет гауссовское распределение, то

$$\left(\frac{S}{N}\right)_{AVE}=\frac{2R}{\sqrt{2\pi}\,\sigma_\Phi}\int\limits_{-\infty}^{\infty}\frac{\exp\left(-\Phi^2/2\sigma_\Phi^2\right)}{1+2R'\,(1-\cos\Phi)^2}\,d\Phi. \tag{9.6}$$

Так как $(1+x)^{-1}\geqslant 1-x$ для всех действительных значений x, то

$$\left(\frac{S}{N}\right)_{AVE}\geqslant\frac{2R}{\sqrt{2\pi}\,\sigma_\Phi}\int\limits_{-\infty}^{\infty}\exp\left(-\frac{\Phi^2}{2\sigma_\Phi^2}\right)\left[1-2R'\,(1-\cos\Phi)^2\right]d\Phi=$$

$$=2R\left[1-3R'+4R'\exp\left(-\frac{\sigma_\Phi^2}{2}\right)-R'\exp\left(-2\sigma_\Phi^2\right)\right]\approx$$

$$\approx 2R\left[1-\frac{3}{2}\,R'\,\sigma_\Phi^4\right]. \tag{9.7}$$

Эта граница в действительности дает хорошую оценку для среднего отношения сигнал/шум только тогда, когда σ_Φ достаточно мало, так что $2R'(1-\cos\Phi)^2\ll 1$ для $|\Phi|\leqslant 3\sigma_\Phi$. Последнее приближение в ф-ле (9.7) справедливо также при этом предположении.

Для того чтобы определить влияние ошибки в выборе длительности (прямоугольного) 1) символа, заметим, что интеграл в ф-ле (9.4), если ошибка синхронизации символов равна τ секунд (в предположении, что частота несущей велика по сравнению с $1/T_s$ так, что несущей можно пренебречь), принимает вид

$$I=\frac{1}{AT_s}\int_{\tau}^{T_s}x_1(t)\,dt+\frac{1}{AT_s}\int_{T_s}^{T_s+\tau}x_2(t)\,dt \tag{9.8}$$

для $\tau\geqslant 0$ и

$$I=\frac{1}{AT_s}\int_{\tau}^{0}x_0(t)\,dt+\frac{1}{AT_s}\int_{0}^{T_s+\tau}x_1(t)\,dt \tag{9.9}$$

для $\tau<0$, где $x_i(t)=Ax_i+n(t)$; $iT_s<t<(i+1)T_s$. Таким образом, если x_0, x_1, и x_2 предполагаются независимыми и одинаково распределенными, то

$$\left(\frac{S}{N}\right)_{\tau}=\frac{\operatorname{var}(x)}{E(I-x)^2}=\left[\frac{2R}{1+4R'\left(\frac{\tau}{T_s}\right)^2}\right]. \tag{9.10}$$

Если ошибка в опорном сигнале $\xi\triangleq\tau/T_s$ имеет гауссовское распределение с нулевым средним и дисперсией σ_ξ^2, то ф-ла (9.1) дает

$$\left(\frac{S}{N}\right)_{AVE}=\frac{2R}{\sqrt{2\pi}\,\sigma_\xi}\int_{-\infty}^{\infty}\frac{\exp\left(-\frac{\xi}{2\sigma_\xi^2}\right)}{1+4R'\xi^2}\,d\xi=\sqrt{\frac{\pi}{2}}\,\frac{R\exp\left(\frac{1}{8R'\sigma_\xi^2}\right)}{(R')^{1/2}\sigma_\xi^2}\times$$

$$\times\left\{1-\operatorname{erf}\left[\frac{1}{2\sigma_\xi(2R')^{1/2}}\right]\right\}\approx 2R\left\{1-4R'\sigma_\xi^2\right\}. \tag{9.11}$$

Таким образом, влияние несовершенства в символьной синхронизации состоит в уменьшении отношения сигнал/шум в $(1-4R'\times\sigma_\xi^2)$ раз. Аналогичные рассуждения приводят к тому же заключению для фазовонекогерентной АИМ, когда R велико (ср. с § 3.6).

Наконец, рассматривая совместно эффекты, возникающие из-за ошибок синхронизации несущей и символов, получаем

$$I=\frac{1}{AT_s}\int_{\tau}^{T_s+\tau}y(t)\sqrt{2}\sin(\omega_c t-\Phi)\,dt. \tag{9.12}$$

---

1) Наиболее частой причиной использования непрямоугольных импульсов является желание сузить спектр сигнала. В результате широко используемые непрямоугольные импульсы имеют более широкие автокорреляционные функции по сравнению с прямоугольными импульсами, и в соответствии с этим система связи, использующая такие импульсы, подвергается меньшему неблагоприятному влиянию за счет неточностей в синхронизации символов. *(Прим. авт.).*

Если $\omega_c \gg 1/T_s$, то

$$\left(\frac{S}{N}\right)_{\Phi\xi} = \left[\frac{2R}{1 + 2R'(1 - \cos\Phi)^2 + 4R'\,|\xi|\cos\Phi\,(1 - \cos\Phi) + 4R'\,\xi^2\cos^2\Phi}\right], \tag{9.13}$$

где обозначения те же, что и ранее. Если σ_Φ и σ_ξ малы, то

$$\left(\frac{S}{N}\right)_{AVE} \approx 2R\left[1 - 4R'\,\sigma_\xi^2 - 2R'\,\sigma_\Phi^2\,\sigma_\xi\left(\sqrt{\frac{2}{\pi}} - 2\sigma_\xi\right) - \frac{3}{2}R'\,\sigma_\Phi^4\right]. \tag{9.14}$$

Только что полученный результат был выведен в предположении, что ошибка синхронизации символов и фазовая ошибка несущей независимы. Часто обе они получаются с помощью одного и того же опорного сигнала. В этом случае $\xi = \Phi/\pi m$, где m — число полупериодов несущей на символ ($\omega_c = \pi m/T_s$). Тогда

$$\left(\frac{S}{N}\right)_{\Phi} = \left\{\frac{1}{2R'} + (1 - \cos\Phi)^2 + 2f(\Phi)\,[f(\Phi) + (1 - \cos\Phi)]\right\}^{-1}\frac{R}{R'}, \tag{9.15}$$

где $f(\Phi) = \frac{1}{\pi m}[\Phi\cos\Phi - \sin\Phi]$. Так как последний член в ф-ле (9.15) имеет порядок $|\Phi^5|/3\pi m$ при малых Φ, а второй член — порядок $\Phi^4/4$, то для разумно малых значений σ_Φ последним членом можно пренебречь независимо от значения m. Это приводит к заключению, что ухудшение характеристики определяется в основном лишь фазовой ошибкой несущей, если синхронизация, как несущей, так и символов получается с помощью одного и того же опорного сигнала [ср. с (9.5)].

Итак, отношение сигнал/шум на выходе для АИМ уменьшается приближенно в

$$\left[1 - 4R'\,\sigma_\xi^2 - 2R'\,\sigma_\Phi^2\,\sigma_\xi\left(\sqrt{\frac{2}{\pi}} - 2\sigma_\xi\right) - \frac{3}{2}R'\,\sigma_\Phi^4\right] \tag{9.16}$$

раз (когда дисперсия фазовой ошибки несущей равна σ_Φ^2, а дисперсия ошибки символьной синхронизации равна σ_ξ^2). Если оба опорных сигнала получаются с помощью одного и того же сигнала, то уменьшение возникает, по существу, лишь из-за фазовой ошибки несущей [это уменьшение определяется ф-лой (9.16) при $\sigma_\xi = 0$].

9.3. Влияние неточностей в опорных сигналах. Фазовая манипуляция

В этом параграфе исследовано влияние неточностей опорных сигналов на характеристики различных ФТ систем, рассмотренных в гл. 3 и 4. Начнем с двоичного случая. Если местная опорная несущая имеет ошибку Φ рад, то математическое ожидание выхода коррелятора приемника (см. § 4.5) равно

$$E(I\mid\Phi)=\frac{1}{AT_s}\int_0^{T_s}(\pm\sqrt{2}\,A\sin\omega_c t)\sqrt{2}\sin(\omega_c t-\Phi)\,dt=\pm\cos\Phi, \qquad (9.17)$$

где, по предположению, $\omega_c=\pi m/T_s$, а m либо равно целому числу, либо велико по сравнению с единицей. Так как дисперсия этого выхода не зависит от Ф, то единственным следствием ошибки при определении опорной несущей является снижение действующей амплитуды сигнала в $\cos\Phi$ раз. Таким образом, если фаза опорной несущей имеет ошибку Ф рад, условная вероятность ошибки в символе равна

$$P_e(\Phi)=\frac{1}{2}\left[1-\operatorname{erf}(R^{1/2}\cos\Phi)\right], \qquad (9.18)$$

где $R=A^2T_s/N_0$ [ср с (4.71)]. Если Ф имеет гауссовское распределение с дисперсией σ_Φ^2, то вероятность ошибки в символе равна

$$P_e=\int_{-\infty}^{\infty}p(\Phi)\,P_e(\Phi)\,d\Phi=\frac{1}{\pi\sigma_\Phi}\int_0^{\infty}\exp\left(-\frac{\Phi^2}{2\sigma_\Phi^2}\right)\times$$

$$\times\int_{\sqrt{2}\,R^{1/2}\cos\Phi}^{\infty}\exp\left(-\frac{y^2}{2}\right)dy\,d\Phi. \qquad (9.19)$$

Эта вероятность была определена численными методами и изображена на рис. 9.1 как функция R для различных значений σ_Φ. Отметим, что при $R\to\infty$ P_e стремится к ненулевой постоянной (которая называется иногда *остаточной вероятностью ошибки*) при любом ненулевом значении дисперсии σ_Φ^2. Увеличение отношения сигнал/шум становится все менее и менее эффективным, не приводя к соответствующему уменьшению ошибки опорного сигнала.

Остаточная вероятность ошибки, конечно, является вероятностью того, что фазовая ошибка в опорном сигнале Ф выходит из интервала $(-\pi/2,\ \pi/2)$ по модулю 2π. Так как гауссовское приближение к распределению Ф, очевидно, становится плохим для значений Ф, превосходящих $\pi/2$ рад, то вероятность ошибки, определяемая (9.19) при $R\to\infty$, будет соответственно менее точной оценкой для истинной вероятности ошибки, чем в случае малых значений R. В общем случае ошибка, возникающая за счет гауссовского приближения, становится ощутимой для значений R, превосходящих $1/(2\sigma_\Phi^2)$, так как вероятность фазовой ошибки, бо́льшей, чем $\pi/2$ рад, при этом перестает быть пренебрежимо малой по сравнению с вероятностью ошибки, обусловленной аддитивным шумом (ср. с задачей 9.1). Этот случай имеет малую практическую ценность, поскольку в правильно построенных системах, как мы знаем, σ_Φ^2 почти всегда меньше, чем $1/(2R)$. Тем не менее некоторые из кривых на рис. 9.1 были продолжены за точку $R=$

$=1/(2\sigma_\Phi^2)$, чтобы дать грубое представление (в общем оптимистическое) о вероятности ошибки, которая могла бы ожидаться, если бы система работала при этих условиях[1].

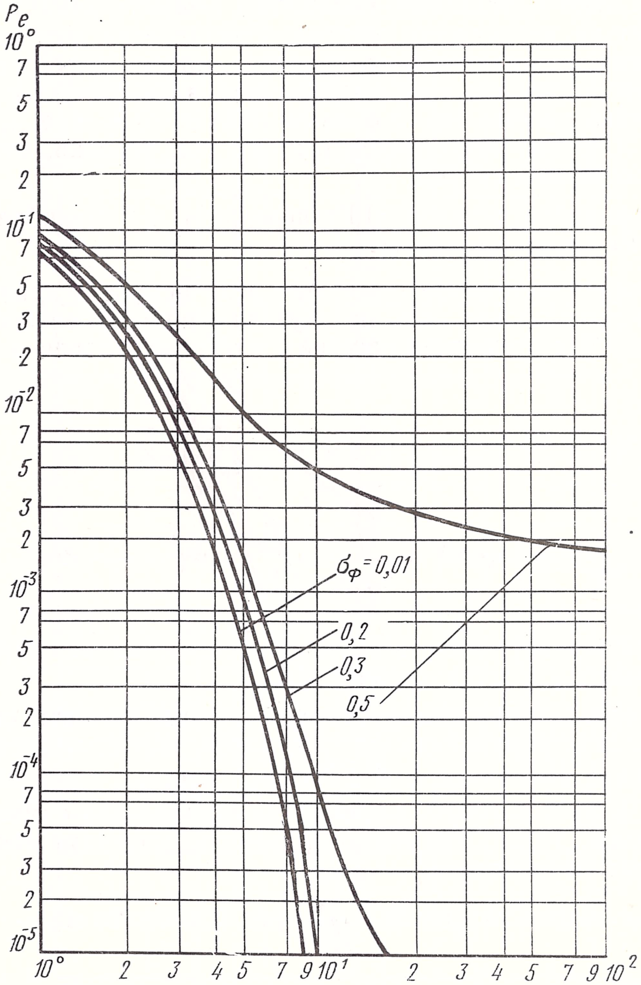


Рис. 9.1. Вероятность ошибки в символе для двоичной ФТ при несовершенной синхронизации несущей

---

[1] Если в качестве опорного сигнала использовать выходной сигнал системы ФАПЧ, то можно было бы использовать вместо гауссовского распределения в (9.19) распределение Тихонова (ср. с задачей 5.5) или подходящее обобщение его для получения, в общем, более точной оценки вероятности ошибки. Однако, кроме некоторых частных случаев (например, системы первого порядка без сдвига частоты), трудности вычисления при анализе увеличиваются во много раз, и в любом случае результаты достаточно хорошо согласуются с теми, которые получаются при гауссовском приближении для всех $\sigma_\Phi^2 \leqslant 1/(2R)$. (*Прим. авт.*).

Влияние ошибки *символьной* синхронизации на вероятность ошибки зависит от наличия или отсутствия перехода символов. Если два последовательных (прямоугольных) символа одинаковы, то неправильное определение положения символа никоим образом не повлияет на вероятность ошибки. Однако если два последовательных символа различны, то величина математического ожидания на выходе коррелятора уменьшается в $1-(2|\tau|/T_s)$ раз, где τ — временна́я ошибка [ср. с ф-лами (9.8) и (9.9) при $x_1=1$, $x_0=x_2=-1$]. Поэтому вероятность ошибки при условии, что задана временная ошибка τ секунд,

$$P_e(\tau)=\mathrm{Pr}(\text{ошибка}\,|\,\text{переход},\ \tau)\,\mathrm{Pr}(\text{переход}\,|\,\tau)+\mathrm{Pr}(\text{ошибка}\,|\,\text{перехода нет},\ \tau)\,\mathrm{Pr}(\text{перехода нет}\,|\,\tau). \tag{9.20}$$

Если последовательные символы независимы и принимают с равными вероятностями одно из двух значений, вероятность перехода равна 1/2 и временная ошибка $\xi=\tau/T_s$ распределена по Гауссу, то

$$P_e=\int\limits_{-\infty}^{\infty}P_e(\tau)\,p(\tau)\,d\tau=\frac{1}{4\pi\sigma_\xi}\int\limits_{-\infty}^{\infty}\exp\left(-\frac{\xi^2}{2\sigma_\xi^2}\right)\times$$

$$\times\int\limits_{(2R)^{1/2}(1-2|\xi|)}^{0}\exp\left(-\frac{x^2}{2}\right)dx\,d\xi+\frac{1}{2\sqrt{2\pi}}\int\limits_{(2R)^{1/2}}^{\infty}\exp\left(-\frac{x^2}{2}\right)dx. \tag{9.21}$$

На рис. 9.2 эта вероятность ошибки изображена как функция R для нескольких различных значений σ_ξ.

Чтобы определить одновременное влияние фазовой ошибки и ошибки сигнала синхронизации символов, допустим, что принимаемый сигнал имеет вид $\pm\sqrt{2}A\sin\omega_c t$, местный опорный сигнал имеет вид $\sqrt{2}\sin(\omega_c t-\Phi)$ и временна́я ошибка для символа равна τ секундам. Тогда, как легко проверить, математическое ожидание выхода коррелятора

$$E(I\,|\,\Phi,\ \xi)=\cos\Phi-2\delta\left\{\xi\cos\Phi-\frac{1}{2\pi m}\left[\sin\Phi+\sin(2\pi m\xi-\right.\right.$$

$$\left.\left.-\Phi)\right]\right\}\mathrm{sgn}(\xi), \tag{9.22}$$

где $\delta=1$, когда имеется переход символов, и $\delta=0$, когда он отсутствует. Здесь вновь $\omega_c=m\pi/T_s$, а m либо равно целому числу, либо $m\gg1$. Если $m\gg1$, то

$$E(I\,|\,\Phi,\ \xi)=(1-2\delta|\xi|)\cos\Phi=E(I\,|\,\Phi)\,E(I\,|\,\xi). \tag{9.23}$$

В противоположность этому предположим, что для установления синхронизации фазы несущей и символьной синхронизации используется один и тот же опорный сигнал. Тогда $\xi=\Phi/\pi m$ и из ф-лы (9.22) имеем

$$E\ (I \mid \Phi,\ \xi) = \cos\Phi - \frac{2\delta}{\pi m}\Big[\Phi\cos\Phi - \sin\Phi\Big] \times \operatorname{sgn}(\Phi). \tag{9.24}$$

Так как $\sin\Phi \geqslant \Phi\cos\Phi$ при $0 \leqslant \Phi \leqslant \Phi_0$, $\Phi_0 > \pi$ и $\sin\Phi \leqslant \Phi\cos\Phi$ при $-\Phi_0 < \Phi \leqslant 0$, $\Phi_0 > \pi$; то ухудшение из-за наличия одновременно символьной ошибки и ошибки в фазе несущей, всегда меньше, чем ухудшение, связанное лишь с ошибкой в фазе несущей. Верхняя граница для случая одновременного участия двух ошибок получается, следовательно, с помощью рассмотрения лишь ошибок в фазе несущей. Для больших значений m отличие этих двух случаев является, конечно, пренебрежимо малым.

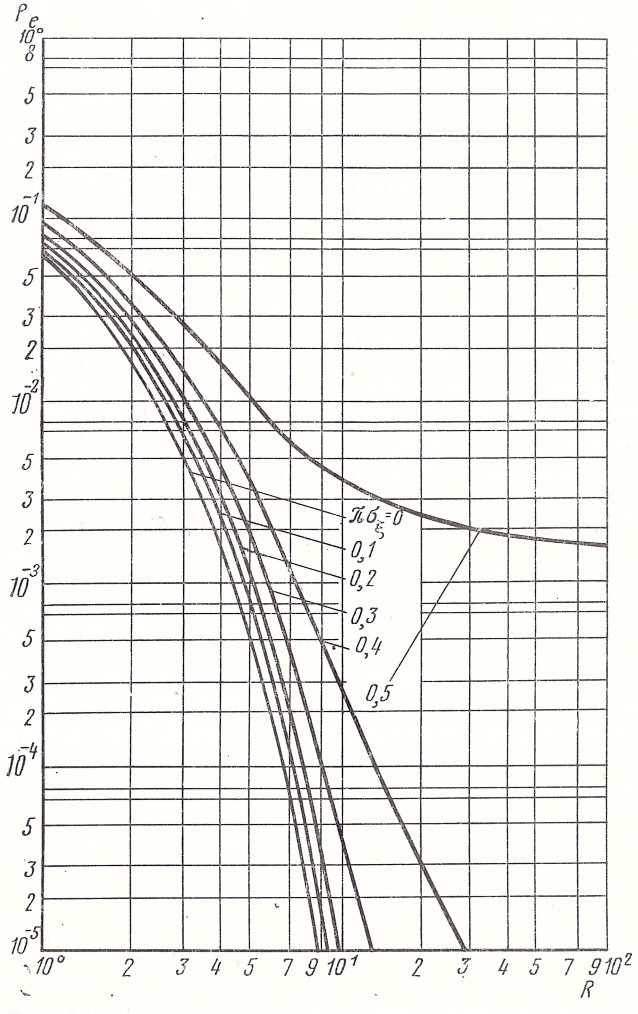


Рис. 9.2. Вероятность ошибки в символе для двоичной ФТ при несовершенной символьной синхронизации

Другой интересный случай возникает, когда вместо синусоидальной используется прямоугольная несущая (поднесущая). В этом случае уменьшение уровня сигнала, вызываемое временной ошибкой τ секунд (если как синхронизация символов, так и синхронизация несущей получаются с помощью одного и того же опорного сигнала),

$$E(I\,|\,\xi) = [1 - 4\,|\,\xi\,| + 4\delta\,|\,\xi\,|/m], \quad \xi \leqslant 1/2, \tag{9.25}$$

где $\xi = \tau/T_0$ и где $T_0 = 2T_s/m$ — период несущей. Отрицательный член связан лишь с фазовой ошибкой несущей. Опять результат, относящийся к одновременным синхронизационным ошибкам, может быть оценен, если пренебречь ошибкой символьной синхронизации. Эта граница быстро сходится к точному выражению при возрастании m.

Вывод аналогичных результатов для q-ичной ФТ при $q > 2$ выполняется с помощью простого (хотя и несколько громоздкого) обобщения предыдущих рассуждений. Этот анализ можно упростить при использовании метода оценки вероятности ошибки из § 4.5. Видоизменяя эти границы применительно к рассматриваемому случаю, найдем, например, что вероятность ошибки в символе для q-ичной ФТ системы при условии, что фазовая ошибка опорной несущей равна Φ, ограничена неравенствами:

$$\frac{1}{2}\{P_0(q;\ \Phi) + P_0(q; -\Phi)\} \leqslant \max\{P_0(q;\ \Phi);\ P_0(q; -\Phi)\} \leqslant$$

$$\leqslant P_e(q;\ \Phi) \leqslant P_0(q;\ \Phi) + P_0(q;\ -\Phi), \tag{9.26}$$

где $P_0(q;\ \Phi) = \frac{1}{2} - \frac{1}{2}\,\mathrm{erf}\,(R^{1/2}\sin(\pi/q - \Phi))$. Средняя вероятность ошибки поэтому хорошо аппроксимируется с помощью выражения (9.19) при замене $\cos\Phi$ на $\sin[(\pi/q) - |\Phi|]$. Аналогично, если ошибка символьной синхронизации равна τ секундам и если разность фаз двух символов, влияющих на некоторое частное решение, равна $\Delta\Phi$ рад, то

$$\frac{1}{2}[P_0(q;\ \tau,\ \Delta\Phi) + P_0(q;\ \tau,\ -\Delta\Phi)] \leqslant P_e(q;\ \tau,\ \Delta\Phi) \leqslant$$

$$\leqslant P_0(q;\ \tau,\ \Delta\Phi) + P_0(q;\ \tau,\ -\Delta\Phi), \tag{9.27}$$

где $P_0(q;\ \tau,\ \Delta\Phi) = \frac{1}{2} - \frac{1}{2}\mathrm{erf}\left\{R^{1/2}\left[(1 - |\,\xi\,|)\sin\frac{\pi}{q} + |\,\xi\,|\sin\left(\frac{\pi}{q} - \Delta\Phi\right)\right]\right\}$

и $\xi = \tau/T_s$. Среднюю вероятность ошибки можно оценить путем усреднения по ξ и $\Delta\Phi$ [ср. с (9.21)]. Заметим, что оценки снизу в (9.26) и (9.27) обращаются в равенства, когда $q = 2$. Более того, когда $q = 4$, эти же самые нижние границы представляют собой вероятности ошибок на *бит,* если фаза опорной синусоиды имеет ошибку Φ, а ошибка символьной синхронизации равна τ. Это утверждение непосредственно следует из рассмотрения § 4.7.

Более простая, хотя и приближенная, мера влияния синхронизационных ошибок в ФТ системе связи получается при использовании приближенного распределения ошибки оценивания фазы, описанного в § 3.7. В частности, если принимаемый сигнал имеет вид $\sqrt{2}A\sin(\omega_c t+\Phi+\Phi_e)+n(t)$, где Φ_e — фазовая ошибка опорного сигнала, то распределение оценки $\hat{\Phi}$ принимаемой фазы можно приближенно представить в виде

$$p(\hat{\Phi}\,|\,\Phi_e)\approx\sqrt{\frac{R}{\pi}}\exp\left[-R\left(\hat{\Phi}-\Phi-\Phi_e\right)^2\right]. \tag{9.28}$$

Следовательно,

$$p\left(\hat{\Phi}\right)\approx\frac{1}{\sqrt{2\pi}\,\sigma}\int\limits_{-\infty}^{\infty}\exp\left[-\frac{\Phi_e^2}{2\sigma_\Phi^2}\right]p\left(\hat{\Phi}\,|\,\Phi_e\right)d\Phi_e\approx\frac{1}{\sqrt{2\pi}\sigma_0}\times$$

$$\times\exp\left[-\frac{\left(\hat{\Phi}-\Phi\right)^2}{2\sigma_0^2}\right], \tag{9.29}$$

где $\sigma^2{}_0=(1+2\sigma_\Phi^2 R)/2R$ и где $\sigma_\Phi^2=E(\Phi^2{}_e)$. Следовательно, неточность фазы опорного сигнала увеличивает дисперсию ошибки оценивания от значения $1/2R$ до значения $\sigma^2{}_0=(1+2\sigma_\Phi^2 R)/2R$ и, следовательно, увеличивает вероятность ошибки от значения

$$P_e(\sigma_\Phi=0)\approx 1-\operatorname{erf}\left(\frac{\pi}{q}R^{1/2}\right). \tag{9.30}$$

до значения

$$P_e(\sigma_\Phi)\approx 1-\operatorname{erf}\left[\frac{\pi}{q}\;\frac{R^{1/2}}{(1+2\sigma_\Phi^2 R)^{1/2}}\right]. \tag{9.31}$$

Это приближение особенно полезно, когда q велико.

Из (9.29) следует также, что среднее отношение сигнал/шум в непрерывной по амплитуде ФТ системе при условии, что имеется фазовая ошибка в опорном сигнале,

$$\left(\frac{S}{N}\right)_{\mathrm{AVE}}=\frac{\pi^2}{3\sigma_0^2}=\frac{\pi^2}{3}\;\frac{2R}{(1+2\sigma_\Phi^2 R)}, \tag{9.32}$$

где σ_Φ^2 — дисперсия этой ошибки опорного сигнала.

Относительная когерентная система ФТ, конечно, не нуждается в фазовокогерентной опорной несущей. Это утверждение может, однако, привести к заблуждению. Если, например, демодуляция выполняется с помощью оценивания последовательных фаз символов и наблюдения разностей фаз [ср. с (4.79)], то, очевидно, заранее предполагается, что имеется в распоряжении точно известная опорная несущая. Хотя установившаяся фаза этого опорного сигнала является несущественной, его кратковременные флуктуации фазы должны быть малыми, в противном случае будет вноситься смещение в оцениваемые разности фаз. Точно также, если используется схема с задержкой, изображенная на рис. 4.5, то эта задержка должна быть весьма точной. Если она будет иметь ошибку ΔT секунд, то при каждом сравнении фаз будет возникать ошибка, дающая смещение $\omega_c \Delta T$ рад. Влияние этих ошибок, а также любых ошибок символьной синхронизации может быть оценено с помощью введения необходимых изменений в соответствующие результаты, относящиеся к когерентной ФТ. Возросшая вероятность ошибки (из-за постоянной ошибки, вызывающей фазовое смещение, или из-за нестабильностей символьной синхронизации) в двоичной относительной когерентной системе, например, может быть определена, если заменить функцию $1-\mathrm{erf}(x)$ на e^{-x^2} в ф-лах (9.18) или (9.21) соответственно. Когда $q>2$, необходимо лишь уменьшить вдвое отношение сигнал/шум в результатах, относящихся к фазовокогерентному случаю, чтобы найти аналогичные выражения для относительного когерентного случая (ср. с § 4.6).

9.4. Влияние неточностей в опорных сигналах. Ортогональные символы

Так же, как и в системах связи, рассмотренных выше, в системе с ортогональными символами основной причиной, приводящей к ухудшению характеристики, вообще говоря, является фазовая ошибка несущей. Это, в частности, верно, когда частота несущей велика по сравнению с обратной величиной периода символа и когда все опорные сигналы, в том числе опорная несущая, получаются на основе одного и того же источника. В силу этого, а также того, что влияние других синхронизационных ошибок сильно зависит от конкретно используемого ортогонального алфавита, ограничимся здесь лишь рассмотрением влияния неточностей опорной несущей.

Предположим, что сигнальный алфавит состоит из множества сигналов единичной энергии

$$s_i(t, \Phi) = \sqrt{2}\,\alpha_i(t)\sin(\omega_c t + \Phi) + \sqrt{2}\,\beta_i(t)\cos(\omega_c t + \Phi), \quad 0 < t < t_s \tag{9.33}$$

[см. (4.26)]. Приемник по принятому сигналу $y(t) = As_r(t, \Phi_0) + n(t)$, $0 < t < T_s$ определяет корреляции

$$I_i = \frac{1}{AT_s}\int_0^{T_s} y(t)\, s_i(t, \Phi_1)\, dt, \tag{9.34}$$

где Φ_1 — оцененная фаза несущей. (Предполагается, что ошибка символьной синхронизации пренебрежимо мала.) Математическое ожидание величины I_i при заданной величине $\Phi = \Phi_0 - \Phi_1$

$$E(I_i \mid \Phi) = \widetilde{\rho}_{ri}\cos\Phi + \hat{\rho}_{ri}\sin\Phi \tag{9.35}$$

[ср. с (4.31), (4.32); как обычно, частота несущей ω_c предполагается достаточно большой для того, чтобы было законным пренебрежение компонентами удвоенной частоты]. Если множество сигналов является ортогональным в фазовонекогерентном смысле, то

$$E(I_i\,|\,\Phi)=\begin{cases}\cos\Phi, & i=r;\\ 0, & i\neq r,\end{cases}\tag{9.36}$$

и фазовая ошибка уменьшает амплитуду сигнала в $\cos\Phi$ раз.

Во многих практических ситуациях, когда приходится рассматривать ошибку опорной несущей, в общем стоит по возможности увеличивать ширину полосы, чтобы выбрать множество сигналов, ортогональное в фазовонекогерентном смысле. Если фазовая ошибка Φ всегда достаточно мала, так, что можно пренебречь членом $\hat{\rho}_{ri}\sin\Phi$, то фазовокогерентная ортогональность возможно будет достаточной. В любом случае математические ожидания выходов корреляторов, по существу, будут такими, как в ф-ле (9.36).

Дисперсия этих выходов, очевидно, не зависит от фазовой ошибки опорного сигнала, так что единственное изменение в характеристике системы возникает из-за снижения эффективной мощности сигнала в $\cos^2\Phi$ раз. Таким образом, из ф-лы (4.11) для средней вероятности ошибки получаем

$$P_e=1-\frac{1}{(2\pi)^{(N+1)/2}\,\sigma_\Phi}\int\limits_{-\infty}^{\infty}\exp\left(-\frac{\Phi^2}{2\sigma_\Phi^2}\right)\int\limits_{-\infty}^{\infty}\exp\left(-\frac{x^2}{2}\right)\times$$

$$\times\left[\int\limits_{-\infty}^{x+\sqrt{2}R^{1/2}\cos\Phi}\exp\left(-\frac{y^2}{2}\right)dy\right]^{N-1}dx\,d\Phi.\tag{9.37}$$

Эта вероятность ошибки изображена на рис. 9.3 как функция $R_b=R/\log_2 N$ для различных N и σ_Φ. Эти кривые (подобно кривым, изображенным на рис. 9.1 и 9.2) дают оценку снизу для P_e, когда вероятность события $\{|\Phi|\geqslant\pi/2\}$ не мала по сравнению с P_e, т. е. когда σ_Φ^2 больше $1/R$. Однако вновь в правильно построенной системе σ_Φ^2 почти всегда будет меньше, чем $1/R$.

Тот же подход, что и для ортогонального множества, очевидно, может быть использован для биортогонального множества сигналов. В силу того что характеристики биортогональной и ортогональной систем близки, когда используется более четырех символов, влияние неточности фазы опорной несущей будет почти одинаковым в этих двух случаях.

Следует подчеркнуть, что результаты, относящиеся к влиянию синхронизационных ошибок на вероятности ошибок в символах, основываются на предположении, что синхронизационные ошибки остаются постоянными в течение любого интервала корреляции. В другом крайнем случае, когда синхронизационные ошибки могут значительно меняться на интервале интегрирования, может оказаться более разумным определить среднюю эффективную мощность сигнала и использовать эту среднюю мощность для оценки

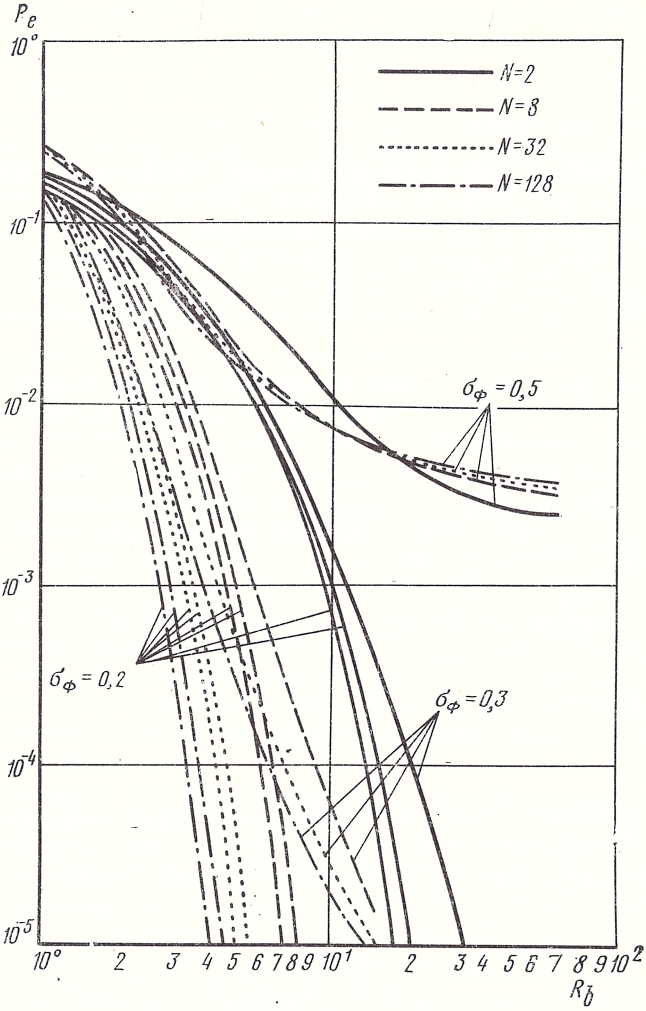


Рис. 9.3. Вероятность ошибки для ортогональных символов при несовершенной синхронизации несущей

вероятности ошибки. Так, например, в только что рассмотренной ситуации средняя амплитуда на выходе правильного коррелятора

$$E(I_r) \approx \frac{1}{\sqrt{2\pi}\,\sigma_\Phi} \int_{-\infty}^{\infty} \exp\left(-\frac{\Phi^2}{2\sigma_\Phi^2}\right) \cos\Phi \, d\Phi = \exp\left(-\frac{\sigma_\Phi^2}{2}\right). \qquad (9.38)$$

При этом мерой ухудшения характеристики будет увеличение вероятности ошибки в символе, когда R уменьшается от значения A^2T_s/N_0 до $(A^2T_s/N_0)\exp(-\sigma_\Phi^2\quad)$. Для одной и той же величины σ_Φ

это ухудшение будет значительно меньшим, чем то, которое определялось ф-лой (9.37). Тем не менее оно более точно отражает изменение вероятности ошибки, когда Φ изменяется быстро.

9.5. Оптимальное распределение мощности

Часто бывает так, что практические соображения определяют мощность, которая может быть выделена передаваемому опорному сигналу. Если это так, то анализ, проведенный в предыдущих параграфах, дает возможность определить необходимые параметры (отношения сигнал/шум или вероятности ошибок) системы связи. Если, однако, другие ограничения являются менее жесткими, то может оказаться возможным изменить долю общей мощности, выделенной синхронизационному каналу. Очевидно, что если вся мощность используется для передачи информации и не делается попытка установить синхронизацию, то система будет работать очень плохо, как и в том случае, если вся мощность используется для синхронизации и ничего не остается для передачи информации. Следовательно, между этими крайними случаями распределения мощности должен существовать промежуточный, когда характеристика системы будет лучше или в крайнем случае не хуже, чем при любом другом распределении мощности между информационными и синхронизационными сигналами.

Целью этого параграфа является получение относительно простых выражений для условия оптимального распределения мощности. Поскольку, как мы уже знаем, наиболее ощутимое влияние на характеристику системы обычно оказывает ошибка опорной несущей, то мы ограничимся рассмотрением задачи распределения мощности между модулированной и немодулированной частями несущей. Опорная несущая будет выделяться из немодулированной несущей отслеживанием с помощью системы ФАПЧ, имеющей ширину полосы шума B_L Гц ($\sigma_\Phi^2 = N_0 B_L / P_s$, где P_s — мощность немодулированной несущей). Обобщение используемых здесь методов на другие задачи распределения мощности осуществляется просто. Если, например, система имеет не только несущую, но и поднесущую и опорные, поднесущая и несущая независимы (если они получаются из одного и того же источника, то опорная поднесущая, по-видимому, будет более точной), то мощность, в общем, может быть удовлетворительно распределена между тремя каналами методом суперпозиции. Мощность, необходимую для немодулированной несущей, можно определить с помощью полученных здесь результатов в предположении, что опорная поднесущая является абсолютно точной. Аналогично эти же результаты можно использовать для отыскания мощности опорной поднесущей в пренебрежении искажениями, вызываемыми неточным знанием несущей. Если оба опорных сигнала являются достаточно точными, какими они и должны быть для того, чтобы система работала удовлетворительно, то эффекты второго порядка, обусловленные одновременным присутствием ошибок в обоих опорных сигналах, обычно пренебрежимо малы с точки зрения задачи оптимального распределения мощности.

Общий метод будет проиллюстрирован исследованием задачи распределения мощности между модулированной и немодулированной несущими для каждой из систем, рассматривавшихся в предыдущих параграфах.

Амплитудно-импульсная модуляция. Записывая величину, обратную к дисперсии фазы, в виде

$$1/\sigma_\Phi^2 = P_s T_s Q/N_0, \tag{9.39}$$

где $Q = (1/T_s B_L)$, получаем

$$R + 1/Q\sigma_\Phi^2 = (P_s + P_m) T_s/N_0 = P_0 T_s/N_0 \triangleq R_0, \tag{9.40}$$

где P_s — мощность немодулированной несущей; P_m — средняя мощность модуляции и P_0 — полная мощность, имеющаяся в распоряжении, по предположению ограниченная. Тогда

$$1 + \frac{1}{Q}\frac{d(1/\sigma_\Phi^2)}{dR} = 0; \tag{9.41}$$

дифференцируя (9.7) (где $R' = R$) при этом условии, находим приближенно условие для экстремума (который, как легко показать, будет максимумом) среднего отношения сигнал/шум:

$$R = \frac{1}{2Q\sigma_\Phi^2}\left\{\left(1 + \frac{4}{3}\frac{Q}{\sigma_\Phi^2}\right)^{1/2} - 1\right\}. \tag{9.42}$$

Если $Q^2 R_0 \gg 1$, то оптимальное отношение мощности несущей к полной мощности

$$P_s/P_0 \approx (3/Q^2 R_0)^{1/3}. \tag{9.43}$$

Отношение мощности синхронизационного сигнала к полной мощности обратно пропорционально Q. Это соотношение, которое будет появляться во всех задачах распределения мощности, является типичным.

Фазовая манипуляция. Приравнивание нулю производной (9.19) по R при условии, что $R + 1/Q\sigma_\Phi^2$ постоянно, дает

$$\int_0^\infty \exp\left(-\frac{x^2}{2}\right)\exp[-R\cos^2(\sigma_\Phi x)]\cos(\sigma_\Phi x)\,dx =$$

$$= R\sigma_\Phi^3 Q\int_0^\infty \exp\left(-\frac{x^2}{2}\right)\exp[-R\cos^2(\sigma_\Phi x)]\,x\sin(\sigma_\Phi x)\,dx. \tag{9.44}$$

Это уравнение также было решено численно. Решение, выраженное как отношение P_s/P_0, представлено на рис. 9.4 как функция R_0 для различных значений Q. Ур-ние (9.44) решается приближенно, если $\sigma_\Phi \ll 1$, т. е. если $\cos\sigma_\Phi x \approx 1 - (\sigma_\Phi^2 x^2/2)$ и $x\sin\sigma_\Phi x \approx x^2\sigma_\Phi$. Пола-

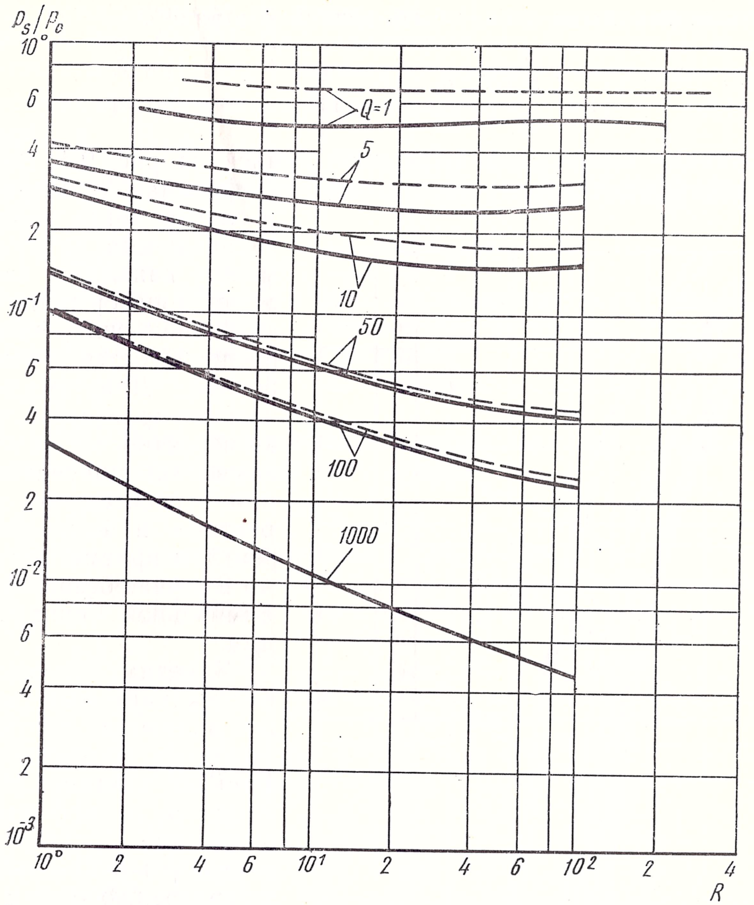


Рис. 9.4. Оптимальное распределение мощности между сигналом двоичной ФТ и несущей

гая $\sigma_x = (1-2\sigma_\Phi^2 R)^{-1/2}$, получаем в этом приближении следующее условие:

$$\frac{2}{\sqrt{2\pi}\,\sigma_x}\int_0^\infty \exp\left(-\frac{x^2}{2\sigma_x^2}\right)dx = \sigma_\Phi^2\left(1+2RQ\,\sigma_\Phi^2\right)\frac{1}{\sqrt{2\pi}\sigma_x}\int_0^\infty x^2 \times$$

$$\times \exp\left(-\frac{x^2}{2\sigma_x^2}\right)dx$$

или

$$1 = \frac{\sigma_\Phi^2}{2}\,\frac{\left(1+2RQ\,\sigma_\Phi^2\right)}{\left(1-2\sigma_\Phi^2 R\right)}\,. \qquad (9.45)$$

Последнее равенство может быть записано в виде

$$\frac{P_s}{P_0}=\frac{1}{\left(R_0-\frac{1}{4}\right)\left[\left(1+\frac{R_0(Q+2)}{(R-1/4)^2}\right)^{1/2}-1\right]}\,. \tag{9.46}$$

Эта функция изображена штриховой линией на рис. 9.4. Вероятность ошибки в символе представлена как функция R_0 на рис. 9.5 в случае, когда мощность распределена оптимально между каналами для несущей и информации; символьная синхронизация предполагается безошибочной. Для сравнения там же приведены графики вероятностей ошибок в символах, получающихся при относительном когерентном и фазовонекогерентном приеме опять-таки в случае безошибочной символьной синхронизации.

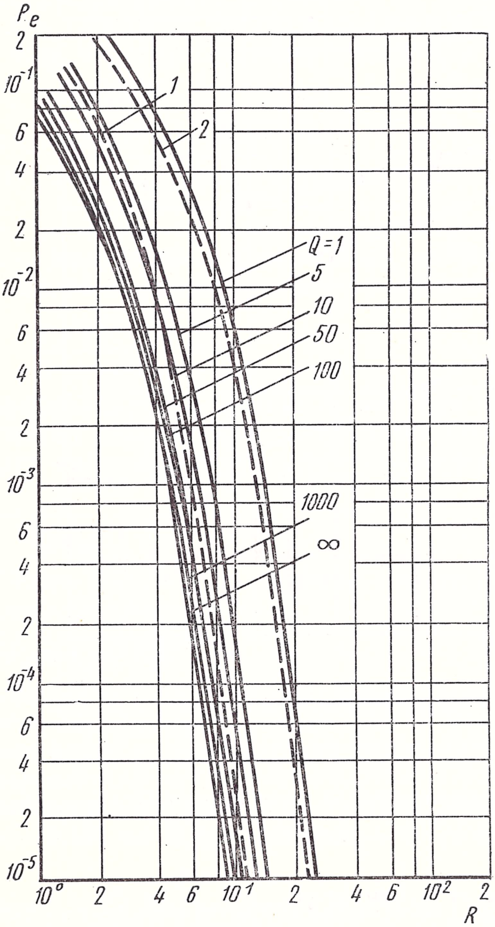


Рис. 9.5. Вероятность ошибки в символе для двоичной ФТ при оптимальном распределении мощности:

1 — относительная когерентная ВИМ; *2* — некогерентная (ортогональная ВИМ)

Заметим, что если два рассматриваемых сигнала не являются противоположными, но имеют коэффициент взаимной корреляции ρ, то эффективное отношение сигнал/шум снижается в (1—ρ)/2 раз по сравнению с этим отношением в случае противоположных сигналов (ср. с гл. 4). Если в предыдущем рассмотрении R заменить на $R(1-\rho)/2=R'$ и Q на $Q'=2Q/(1-\rho)$, то, как легко видеть, приведенные результаты справедливы для произвольного ρ.

Тот же самый подход можно применить для вероятностей ошибки при $q>2$ [т. е. для (9.26)], но вычисления будут громоздкими, а результаты не очень поучительными. Вместо этого перейдем прямо к приближенным выражениям, получающимся из ф-лы (9.29). Как для дискретной, так и для непрерывной по амплитуде ФТ цель распределения мощности в условиях используемого приближения состоит в минимизации дисперсии σ^2_0 [см. (9.29)]. Дифференцируя это выражение по R при условии, что $R+(1/Q\sigma^2_\Phi)$ постоянно, получаем следующее условие экстремума среднего отношения сигнал/шум:

$$2\sigma^4_\Phi QR^2 = 1. \tag{9.47}$$

Следовательно, отношение мощности несущей к полной мощности

$$\frac{P_s}{P_0} = \frac{1}{1+(Q/2)^{1/2}}. \tag{9.48}$$

Заметим, что, когда Q велико по сравнению с R_0, оптимальное распределение мощности в двоичном случае приводит к следующему выражению для мощности несущей:

$$P_s \approx P_0/R_0^{1/2}Q^{1/2} \tag{9.49}$$

[ср. с (9.46)]. В противоположность этому, если число фаз q велико, мощность несущей в тех же условиях

$$P_s \approx P_0/(Q/2)^{1/2} \tag{9.50}$$

[ср. с (9.48)], что дает увеличение в $(2R_0)^{1/2}$ раз.

Ортогональные символы. Дифференцирование выражения (9.37) при условии, что $R+(1/Q\sigma_\Phi^2)$ постоянно, дает

$$\frac{dP_e}{dR} = -\frac{1}{\sqrt{2\pi}} \int\limits_{-\infty}^{\infty} \exp\left(-\frac{z^2}{2}\right) \frac{1}{(2R)^{1/2}} \left[\cos\sigma_\Phi z - R\,\sigma^3_\Phi Qz \sin\sigma_\Phi z\right] \times$$
$$\times \left[\left\{\frac{d}{da} P_N(a)\right\}_{a=\sqrt{2}R\cos\sigma_\Phi z}\right] dz, \tag{9.51}$$

где

$$P_N(a) = \frac{1}{(2\pi)^{N/2}} \int\limits_{-\infty}^{\infty} \exp\left(-\frac{x^2}{2}\right) \left[\int\limits_{-\infty}^{x+a} \exp\left(-\frac{y^2}{2}\right) dy\right]^{N-1} dx.$$

Оптимальное распределение мощности, в принципе, определяется путем приравнивания этого выражения нулю и решения получающегося уравнения относительно σ^2_Φ, что даст возможность выразить σ^2_Φ через R. Численное решение (расчет), однако, весьма громоздко [1]. Однако с помощью некоторых приближений можно получить относительно простое аналитическое выражение для оптимального распределения мощности. Будет показано, что результаты хорошо согласуются с результатами более точного численного решения для всех отношений сигнал/шум, представляющих интерес.

---

[1] В другом численном методе фиксируется полная мощность и для нее вычисляется P_e при различных значениях R и σ^2_Φ. Расчет может быть выполнен и графически путем нанесения на кривых рис. 9.3 геометрического места точек, соответствующих фиксированной полной мощности, что относительно просто для любых заданных множеств параметров N, R_0 и Q. *(Прим. авт.)*.

Начнем с замечания, что для достаточно больших значений a

$$\frac{d}{da} P_N(a) \approx (N-1) \frac{d}{da} P_2(a). \tag{9.52}$$

Это заключение подтверждается рис. 4.2, из которого следует, что скорость изменения вероятностей ошибок (с точностью до постоянного множителя) не зависит от N. Чтобы обосновать это аналитически, заметим, что

$$P_N(a) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} \exp\left(-\frac{x^2}{2}\right)\left[1 - \frac{1}{2}\operatorname{erfc}\frac{x+a}{\sqrt{2}}\right]^{N-1} dx \approx$$

$$\approx \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} \exp\left(-\frac{x^2}{2}\right)\left[1 - \frac{N-1}{2}\operatorname{erfc}\frac{x+a}{\sqrt{2}}\right] dx, \tag{9.53}$$

где

$$\operatorname{erfc}\frac{a+x}{\sqrt{2}} \overset{\Delta}{=} 1 - \operatorname{erf}\frac{x+a}{\sqrt{2}} = 1 - \frac{1}{\sqrt{2\pi}} \int_{-(x+a)}^{x+a} \exp\left(-\frac{y^2}{2}\right) dy.$$

Приближение в ф-ле (9.53) справедливо, когда a велико и, следовательно, $\operatorname{erfc}[(x+a)/2]$ мало для всех x, для которых $\exp(-x^2/2)$ значительно больше нуля. Тогда

$$\frac{dP_N(a)}{da} \approx (N-1)\frac{d}{da}\left\{-\frac{1}{2\sqrt{2\pi}} \int_{-\infty}^{\infty} \exp\left(-\frac{x^2}{2}\right) \times \right.$$

$$\left. \times \operatorname{erfc}\left(\frac{x+a}{\sqrt{2}}\right) dx \right\} = (N-1)\frac{dP_2(a)}{da} \tag{9.54}$$

и из ф-лы (9.51) получаем

$$\frac{dP_e}{dR} \approx -\frac{(N-1)}{\sqrt{2\pi}} \int_{-\infty}^{\infty} \exp\left(-\frac{z^2}{2}\right) \frac{1}{(2R)^{1/2}} [\cos\sigma_\Phi z - R\sigma_\Phi^3 Qz \sin\sigma_\Phi z] \times$$

$$\times \left[\left\{\frac{d}{da} P_2(a)\right\}_{a=\sqrt{2R}\cos\sigma_\Phi z}\right] dz. \tag{9.55}$$

Приравняв это выражение нулю, легко видеть, что полученное равенство не зависит от N. Так как при $N=2$ оптимальное распределение мощности получается, когда удовлетворяется (9.44) (где R заменяется на $R/2$, а Q на $2Q$, так как здесь $\rho=0$), то оно является хорошим приближением к оптимальному распределению мощности для всех значений N. Но так как выражение (9.46) является приближенным решением ур-ния (9.44), справедливым, когда $\sigma_\Phi \ll 1$, то оно применимо и для всех N при том же самом условии. (Здесь также R_0 следует заменить на $R_0/2$, а Q на $2Q$.)

Следует отметить, что параметр R является отношением энергии сигнала, приходящейся на *символ*, к спектральной плотности шума. Как было указано в гл. 4, R должно возрастать пропорционально $\log_2 N$, если вероятность ошибки должна оставаться постоянной при увеличении N. Кроме того, если скорость в битах $1/T_b$ фиксируется, то величина $Q=1/B_L T_s=1/B_L T_b \log_2 N$ будет обратно пропорциональна $\log_2 N$. Так как Q должно быть большим для справедливости предположения относительно постоянства опорной фазы на любом интервале интегрирования, то ограничение на B_L становится более жестким с увеличением N; B_L должно быть малым по сравнению с $1/T_s=1/T_b \log_2 N$.

В заключение отметим, что приведенные выше рассуждения могут быть использованы, по существу, без всякого изменения для биортогонального, а не ортогонального множества сигналов. Оптимальное распределение мощности остается, по существу, таким же.

9.6. Сравнение синхронизации по отдельному каналу с синхронизацией в случае единого канала

Эта глава посвящена исследованию влияния неточностей опорных сигналов синхронизации на характеристику различных систем связи, а также задаче распределения мощности между синхронизационным и информационным каналами. Вместе с тем в гл. 7 и 8 были исследованы несколько методов получения этой синхронизационной информации непосредственно из сигнала, модулированного информацией. Теперь можно определить эффективность этих методов на основе результатов настоящей главы. В этой связи сразу же возникают два вопроса: хуже ли синхронизационные оценки, получаемые непосредственно из модулированного сигнала, чем те, которые получаются с помощью отдельных каналов при оптимальном распределении мощности? Выгодно ли дополнять эти оценки оценками, производимыми в отдельном канале, если вообще это возможно сделать? Вообще говоря, ответы на эти вопросы являются отрицательными.

Для того чтобы обосновать это утверждение, нужно лишь сравнить дисперсии этих двух оценок. Пусть σ^2_1 будет дисперсией синхронизационной оценки, получаемой непосредственно из модулированного сигнала, а σ^2_2 — дисперсией соответствующей оценки, получаемой с помощью второго канала при оптимальном распределении мощности. Заметим, что

$$\frac{1}{\sigma_2^2}=\frac{P_s}{P_0}QR_0 \qquad (9.56)$$

и так как оптимальное отношение P_s/P_0 в каждом из случаев, как было показано, порядка Q^{-r}, где $0<r<1$, то $1/\sigma^2_2$ будет порядка Q^s, где $0<s<1$. В противоположность этому $1/\sigma^2_1$, как было показано в гл. 8, неизменно прямо пропорционально Q. Очевидно, что если $Q=1/B_L T_s$ достаточно велико, то оценка, получаемая непосредственно из передаваемых данных, будет лучше.

Практически выражение «достаточно велико», в общем, охватывает все представляющие интерес значения Q. Так, например, обратное значение дисперсии опорной несущей АИМ, передаваемой по отдельному каналу, в оптимальном случае равно

$$1/\sigma_2^2 = (3QR_0^2)^{1/3} \tag{9.57}$$

[см. (9.43)]. Обратная величина дисперсии оценки с помощью системы Костаса или квадратичной системы

$$1/\sigma_1^2 \approx QR_0^2/(R_0 + 1) \tag{9.58}$$

[см. (8.60)]. Таким образом, последняя оценка лучше, если

$$Q > \sqrt{3}\,(R_0 + 1)^{3/2}/R_0^2. \tag{9.59}$$

Выражение в правой части этого неравенства стремится к нулю при R_0, стремящемся к бесконечности, и равно лишь $2\sqrt{6}$, когда $R_0=1$. Системы Костаса и связанные с ними устройства были рассмотрены в предположении, что $B_L \ll 1/T_s$. Следовательно, эти системы имеют очевидное превосходство, по крайней мере, при рассмотрении опорной несущей АИМ для всех значений Q, для которых справедлив проведенный ранее анализ.

Аналогично в случае синхронизации несущей для двоичной ФТ система Костаса будет давать более точный опорный сигнал, если

$$Q > 5/2R_0 - 3/2R_0^2 + 1/R_0^3. \tag{9.60}$$

Если, например, вероятность ошибки должна быть 10^{-3}, то R_0 должно быть порядка 5 и использование системы Костаса более выгодно для любых Q, больших, скажем, чем 0,57. Для того чтобы провести сравнение этих двух методов более наглядно, график вероятности ошибки в символе, относящийся к случаю, когда опорная несущая получается с помощью системы Костаса, изображен на рис. 9.6. Его следует сравнить с соответствующими кривыми на рис. 9.5. Кроме случая малых отношений сигнал/шум, метод, использующий системы Костаса, приводит к результатам, которые совпадают или лучше результатов для относительной когерентной схемы при всех $Q \geqslant 2$. Интересно отметить, что характеристика, которая получается при использовании оптимальной системы отслеживания ФТ несущей из § 8.3 вместо системы Костаса, по существу, совпадает (при $Q=2$) с характеристикой, получающейся при относительном когерентном приеме для любых отношений сигнал/шум. Если $Q=2$, имеем $B_L=(1/2T_s)$, и ширина полосы системы отслеживания равна ширине полосы T_s-секундного интегратора. Следовательно, почти полная эквивалентность этих двух результатов не должна удивлять. Однако рассмотрения § 8.3, равно как и предположение о гауссовском распределении фазовой ошибки, в лучшем случае являются лишь приближенными, если $Q=(B_LT_s)^{-1}$ невелико. В любом случае ухудшение характеристики при использовании системы Костаса для получения опорной несущей пренебрежимо мало даже для сравнительно малых значений Q.

Сравнимые результаты получаются и для других систем модуляции и других задач синхронизации, рассмотренных выше. Ухудшение характеристики бифазной ФТ системы вследствие несовершенства (прямоугольной) символьной синхронизации, например, оказывается малым (при $R<10$), если среднеквадратическое отклонение синхронизационной ошибки $\sigma_\Phi \overset{\Delta}{=} 2\pi\sigma_\xi$ равно или меньше 0,2 рад (рис. 9.2). Дисперсия ошибки системы отслеживания символов (§ 7.6), как было показано [см. (7.86)], равна

$$\sigma_\xi^2 = \frac{1}{2Q}\left(\frac{\Delta t/T_s}{1-\Delta t/T_s}\right)\left[\left(1-\frac{3\Delta t}{4T_s}\right)\frac{1}{R}+\frac{1}{2R^2}\right]. \tag{9.61}$$

Так как сигнал ошибки линеен в области $|\tau| \leqslant \Delta t/2$, то отношение $\Delta t/T_s$ может быть порядка 1/6, когда $\sigma_\xi = 0{,}1/\pi$ без нарушения условий § 7.6. Таким образом, если $R=5$, то стандартное отклонение синхронизационной ошибки может быть порядка 0,2 рад при $Q\approx 20$.

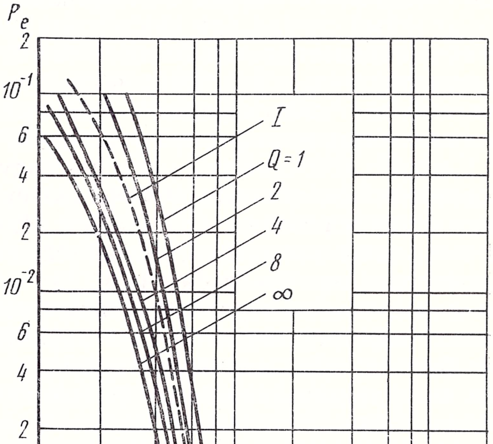


Рис. 9.6. Вероятность ошибки в символе для двоичной ФТ при использовании системы Костаса для получения опорной несущей

Для ответа на второй вопрос о том, стоит ли использовать отдельный синхронизационный канал во вспомогательных целях, заметим, что если синхронизация по единому каналу является более точной по сравнению с синхронизацией по отдельному каналу, когда мощность распределена оптимально, то вообще не следует выделять никакой мощности синхронизационному каналу. Предположим, что оба метода (синхронизации по единому каналу и по отдельному каналу) были использованы одновременно. Если бы объединенная оценка была лучше, чем оценка при использовании отдельного канала с оптимальным распределением мощности, то характеристика системы, очевидно, могла бы быть улучшена с помощью выделения большей мощности информационному каналу, так как синхронизационная оценка ухудшается при таком перераспределении мощности даже менее быстро, чем в случае, когда для получения этой оценки используется лишь синхронизационный канал. И так как характеристика могла бы улучшиться с помощью такого перераспределения мощности, когда имеется возможность использовать лишь одну оценку, это утверждение должно оставаться справедливым, когда используются обе оценки. Таким образом, характеристика системы будет улучшаться по мере перераспределения мощности от канала синхронизации к информационному каналу, по крайней мере, до тех пор, пока опорная синхронизация не перестанет быть более точной, чем при использовании лишь отдельного канала с оптимальным распределением. Но если сам опорный сигнал при синхронизации по единому каналу в действительности является более точным, чем эта величина, то каналу синхронизации не нужно выделять вообще никакой мощности. Поэтому в такой ситуации отдельный синхронизационный канал не может быть использован с выгодой.

Следует подчеркнуть, что предыдущие замечания относились к сравнительному анализу качества синхронизационных оценок по отдельному и по единому каналам. Интересной мерой качества являются, чаще всего, конечно, отношение сигнал/шум на выходе и вероятность ошибки в символе. Так как в случае единого канала вся находящаяся в распоряжении мощность используется для передачи информации, то полная характеристика такой системы может быть лучше, чем характеристика системы с отдельным каналом даже тогда, когда более точная синхронизация получается при использовании отдельного канала. В любом случае, когда Q велико, оба метода синхронизации приводят к почти оптимальной характеристике, и решение относительно того, какой из них должен быть использован, будет основываться на других соображениях. Например, при использовании единого канала не возникают трудности при уплотнении, и поэтому он может быть легче реализован. Вместе с тем абсолютная опорная фаза, которая получается при использовании отдельного канала, могла бы сделать его более привлекательным, так как без него нужен некоторый другой метод для устранения возможных неоднозначностей в информационных последовательностях (ср. с § 8.2 и 8.3).

9.7. Заключительные замечания

Основные выводы из результатов этой главы могут быть сформулированы следующим образом:

1. В когерентной системе, в которой восстанавливаемая несущая служит также для отсчета времени в приемнике, фазовая ошибка несущей является определяющим фактором ухудшения характеристики. В некогерентной системе, в которой отсутствуют вы-

сокочастотные временные отсчеты, или в когерентной системе, в которой символьная синхронизация не связана с опорной несущей, ошибка символьной синхронизации также может иметь значение. В действительности наличие относительно точного отсчета времени может быть главным достоинством когерентной системы по сравнению с некогерентной.

2. Однако даже для умеренно больших значений параметра $Q=1/B_LT_s$ влияние неточностей опорных синхросигналов будет относительно небольшим. В частности, это верно, когда синхронизация получается непосредственно из модулированного сигнала, однако утверждение также остается в силе, когда используется отдельный синхронизационный канал с соответствующим распределением между двумя каналами имеющейся в распоряжении мощности.

3. За исключением случая довольно малых значений параметра Q синхронизация, получаемая непосредственно из модулированного сигнала, заведомо лучше синхронизации, получаемой с помощью отдельного канала при оптимальном распределении мощности.

Рассмотрения этой главы всегда подразумевали использование демодуляторов из гл. 3 и 4. Как было показано, эти демодуляторы оптимальны при совершенной символьной синхронизации, а в случае когерентного приема также и совершенной синхронизации несущей. Интересным обобщением этих результатов было бы определение вида оптимального приемника, в котором учитываются неизбежные неточности синхронизации. В общем случае эта задача оказывается довольно сложной и, с точки зрения результатов настоящей главы, отчасти представляющей академический интерес. Однако в некоторых частных случаях ответы могут быть получены, и они являются наглядными и поучительными.

ЧАСТЬ III

КОДИРОВАНИЕ

Глава 10

КОДИРОВАНИЕ ИСТОЧНИКА. ОДНОЗНАЧНОСТЬ ДЕКОДИРОВАНИЯ

10.1. Введение

При рассмотрении в гл. 4 систем передачи данных предполагалось, что имеется возможность представления информации в виде последовательности дискретных по амплитуде символов. Наиболее простым методом превращения информации (если она не дискретна с самого начала) в такую форму служит дискретизация по времени сообщения на выходе источника и квантование выбранных значений; частота выборок и шаг квантования определяются величиной допустимой ошибки. При этом подходе неизбежны некоторые ограничения. Например, число уровней квантования и, следовательно, результирующее число символов могут быть больше, чем число сигналов, используемых в системе связи. Кроме того, такое представление сообщения может не быть особенно эффективным, поэтому часто целесообразно кодировать информацию, т. е. отображать ее в некоторое более удобное множество символов, которые будем называть *кодовыми символами* (источника).

Один из распространенных методов уменьшения (или в некоторых случаях увеличения) числа различных символов, необходимых для представления информации, называется *импульсно-кодовой модуляцией* (ИКМ). (Термин «Модуляция» в этом названии в известной мере вводит в заблуждение, так как здесь не делается никаких предположений относительно конкретных сигналов, используемых для представления информации.) Предположим, что информационные выборки квантуются на N уровней, а сигнал на выходе модулятора представляет собой один из r возможных сигналов. Тогда каждую выборку можно представить в виде последовательности $\log_r N$ (или наименьшего целого числа, большего, чем $\log_r N$) r-ичных символов. (Если r больше, чем N, то в каждый кодовый символ можно отобразить несколько выборок). Тем самым *алфавит источника* (т. е. множество символов, представляющих информацию) *согласуется с алфавитом канала* (ср. с гл. 1). Интересен также другой метод, который называется *дельта-модуляцией* и состоит в увеличении частоты выборок до такой величины, когда становится возможным представить каждую выборку лишь одним r-ичным символом (в этом случае $r=2$), указывающим знак разности между текущей и предшествующей выборками. Очевидно возможны многочисленные разновидности обоих этих методов.

Даже после того, как источник был согласован с каналом (или, возможно, до этого), возникает необходимость в дальнейших преобразованиях. В гл. 4 обычно предполагалось, что последовательные символы на входе модулятора были независимыми и с равными вероятностями принимали значение любого символа из алфавита. К сожалению, источники редко работают таким образом. Чем больше источник отличается от этой идеальной модели, тем меньшую эффективность имеет система в целом, если не предпринимаются какие-либо меры для компенсации этого отклонения.

Одна из причин несоответствия реальных источников и идеальных моделей состоит в том, что в большинстве источников различные символы появляются на выходе с разными вероятностями. Для иллюстрации получающейся невысокой эффективности предположим, что алфавит источника состоит из четырех символов a, b, c и d, появляющихся с вероятностями $P(a)=1/2$, $P(b)=1/4$, $P_c=$ $=P(d)=1/8$. Эти символы можно, конечно, представить с помощью четырех двоичных последовательностей длины два: 00, 01, 10 и 11; при этом для каждого символа источника требуются два двоичных кодовых символа. Однако если отобразить a в 1, b в 01, c в 001 и d в 000, то для половины символов источника потребовалось бы три кодовых символа, но среднее число кодовых символов, необходимых для представления символа источника, было бы равно $\frac{1}{2}\cdot 1+\frac{1}{4}\cdot 2+\frac{1}{8}\cdot 3+\frac{1}{8}\cdot 3=1\frac{3}{4}$, что дает сокращение на 12,5% по сравнению с первым методом. Отсюда возникает предложение использовать такое соответствие между вероятностью каждого символа и числом кодовых символов для его представления, когда более вероятным символам источника относят более короткие последовательности кодовых символов. Алгоритм фактической минимизации среднего числа кодовых символов, необходимых для представления символа источника, описан в § 10.3.

Второй недостаток реальных источников (по сравнению с идеальными) состоит в почти неизбежной зависимости между последовательными выходными символами источника. Часто источник можно моделировать с помощью *марковского источника* конечного порядка; марковский источник n-го порядка определяется как источник, в котором распределение вероятности текущего выходного символа при условии, что заданы все прошлые выходные символы, является функцией лишь n предыдущих выходных символов. Если марковский источник n-го порядка способен производить N различных выходных символов, то для полного описания статистических свойств текущего выходного символа необходимы N^n условных распределений; в этом случае говорят, что источник имеет N^n возможных *состояний*. Однако, какой бы ни была эта зависимость между выходными символами источника, она означает, что последовательность сообщений содержит избыточность. Каждый символ переносит меньше информации, чем он способен переносить, так как до некоторой степени он предсказуем по предыдущим символам. Имеется целый ряд схем для уменьшения этой избыточности в выходных символах источника и, следовательно, для уменьшения среднего числа символов, необходимых для представления сообщения. Эти схемы обычно называются схемами для *устранения избыточности в сообщении* или для *сжатия данных*.

Другие ограничения, такие, как ограничение на сложность оборудования, на простоту кодирования и декодирования, требование сохранить некоторый определенный порядок отображения символов источника в кодовые символы также в большей или меньшей степени, влияют на выбор метода кодирования. При любом критерии выбора некоторого конкретного кодирования, однако, всегда каждый выходной символ источника (или каждая последовательность выходных символов) представляется последовательностью кодовых символов[1]. Так как в общем случае для каждого выходного символа источника требуется более одного кодового символа, то по необходимости кодовые символы объединяются в *слова;* каждое слово состоит из нескольких символов. Множество допустимых слов называется *кодовым словарем* (источника).

Чтобы словарь имел какой-то практический смысл, он должен удовлетворять одному важному требованию — условию *однозначной декодируемости*. Последовательность слов из словаря D однозначно декодируема или просто *декодируема* тогда и только тогда, когда ее невозможно интерпретировать как некоторую другую последовательность слов того же самого словаря. Словарь D декодируем тогда и только тогда, когда каждая конечная последовательность слов из D декодируема. Это понятие лучше всего проиллюстрировать на примере словаря, который не имеет этого свойства, как, например, словарь $\{w_1=0,\ w_2=10,\ w_3=1001\}$. Невозможно определить, является ли последовательность символов 10010 последовательностью слов w_3w_1 или же слов $w_2w_1w_2$. Этот словарь не является однозначно декодируемым и, следовательно, не может быть использован на практике. (Можно было бы возразить, что между словами всегда можно поместить «пустой интервал», и это гарантирует их декодируемость даже, если словарь неоднозначно декодируем. Но если декодер способен отличать интервал от других символов, то интервал также может быть использован как символ. Использование этого символа-интервала только для разделения слов обычно не является оптимальным, как будет показано.)

Хотя любая конечная последовательность слов однозначно декодируемого словаря может быть декодирована лишь одним спо-

---

[1] Если, как это предполагается здесь, выходные символы источника объединяются в блоки до кодирования и при этом каждый блок содержит заранее определенное число выходных символов, то получающийся код иногда называют *блоковым кодом*. Зарезервируем, однако, этот термин для более ограниченного класса кодов, в котором каждое *кодовое* слово также содержит одно и то же число кодовых символов. *(Прим. авт.)*.

собом, отсюда не следует, что *текущая* последовательность слов обладает этим свойством. Как следствие, может понадобиться некоторая задержка прежде, чем окажется возможным декодирование некоторой последовательности слов. Рассмотрим, например, словарь $D=\{101, 00110, 10111, 11001\}$. Последовательность слов 10111, 00110, 11001 нельзя отличить от последовательности
101, 11001, 10110, 00110,
пока не будет получен пятнадцатый символ. Словарь D является декодируемым, но для однозначного опознавания первого кодового слова может понадобиться пятнадцать (или более) символов. Число d_c символов в самой длинной последовательности слов декодируемого словаря, необходимое для однозначного декодирования первого слова этой последовательности, называется *задержкой декодирования.*

Задержка декодирования декодируемого словаря не обязательно является конечной, как показывает словарь $D'=\{101, 00111, 10111, 11001\}$. Можно показать, что этот словарь является декодируемым. Тем не менее последовательность 101110011100111... может быть декодирована как 101, 11001, 11001, ... или как 10111, 00111, 00111, ... Длина самой длинной неоднозначной последовательности в этом случае неограничена.

Существует множество различных ограничений, которые могут быть наложены на кодирование источника, однако результирующие словари должны во всех случаях быть декодируемыми, для того чтобы иметь практическую ценность. Исходя из этого, большая часть главы посвящена исследованию свойства декодируемости произвольных словарей, а не рассмотрению некоторых частных словарей. Единственным исключением является § 10.3, где, как уже было упомянуто, приведен алгоритм минимизации среднего числа кодовых символов, необходимых для представления символа источника, когда известны вероятности этих символов.

10.2. Неравенство Крафта и полные словари

Приведем необходимое и достаточное условие существования декодируемого словаря, имеющего N слов с длинами (числами кодовых символов) $l_1, l_2, \ldots, l_N$. Начнем с необходимого условия.

Теорема 10.1. Если словарь из N r-символьных слов с длинами $l_1, l_2, \ldots, l_N$ является однозначно декодируемым, то

$$\sum_{i=1}^{N} r^{-l_i} \leqslant 1. \qquad (10.1)$$

(Это неравенство часто называется неравенством *Крафта* или *Крафта—Сцилларда.*)

То, что это неравенство может обращаться в равенство для некоторых декодируемых словарей, почти очевидно, так как словарь, для которого $l_i=l$ $(i=1, 2, \ldots, N)$, является декодируемым, если все кодовые слова различны. Условие $\sum_{i=1}^{l} r^{-l} = Nr^{-l} = 1$ просто приравнивает N величине r^l. Так как имеются в точности r^l различных l-последовательностей из r символов, то условие равенства может удовлетворяться для декодируемого словаря. То, что кодовые словари существуют для *всех* множеств чисел l_i, удовлетворяющих неравенству, может показаться более удивительным.

Последовательность p, состоящая из r-ичных символов, называется *префиксом* слова w, если $w = ps$, где s — некоторая последовательность, содержащая один или более символов. Соответственно последовательность s называется *суффиксом* слова w. Определим кодовый словарь со *свойством префикса,* как словарь, в котором никакое кодовое слово не является префиксом никакого другого кодового слова. Если словарь имеет свойство префикса, то каждое кодовое слово может быть однозначно декодировано сразу же после того, как оно полностью принято. Такие словари называются *мгновенно декодируемыми.* (Требование еще более короткой задержки, т. е. требование, чтобы самые длинные слова можно было декодировать еще до того, как они были полностью приняты, очевидно, было бы непрактичным; если бы оно было возможным, то окончания этих слов, не необходимые для декодирования, могли бы быть опущены в самом начале). Очевидно, для того чтобы словарь был мгновенно декодируемым, он должен обладать свойством префикса. Эти два термина являются синонимами. Сформулируем теперь теорему о том, что словари со свойством префикса и, в силу этого, декодируемые словари со словами, имеющими длины $\{l_i\}$, $(i = 1, 2, \ldots, N)$, существуют для всех множеств $\{l_i\}$, удовлетворяющих условию (10.1).

Теорема 10.2. Для любого множества $\{l_i\}$, удовлетворяющего условию $\sum_{i=1}^{N} r^{-l_i} \leqslant 1$, существует словарь со свойством префикса, использующий r-символьный алфавит и состоящий из кодовых слов с длинами $l_1, l_2, \ldots, l_N$.

Рассмотрим пример: $r = 2$, $l_1 = 1$, $l_2 = 2$, $l_3 = 3$, $l_4 = l_5 = 4$. Тогда $\sum_{i=1}^{5} 2^{-l_i} = 1$ и словарь, обладающий свойством префикса, существует. Все словари (10.2) действительно обладают свойством префикса, а длины их слов удовлетворяют указанному необходимому условию:

1	1	1	1	0	0	0	0
01	01	00	00	10	10	11	11
001	000	011	010	110	111	100	101
0001	0010	0100	0110	1110	1101	1011	1001
0000	0011	0101	0111	1111	1100	1010	1000

. (10.2)

Интересно, что декодируемые словари не только не обязаны быть однозначными для любого множества допустимых длин слов, но даже при дополнительном свойстве префикса словари могут быть реализованы многими способами. Действительно, имеется $\binom{r}{n_1}$ способов выбора первых n_1 слов, $\binom{r^2-rn_1}{n_2}$ способов выбора следующих n_2 слов и т. д., так что общее число мгновенно декодируемых словарей (здесь L — наибольшая из длин слов)

$$N\{l_i\} = \binom{r}{n_1}\binom{r^2-rn_1}{n_2}\binom{r^3-r^2n_1-rn_2}{n_3}\ \ldots$$
$$\ldots\binom{r^L-r^{L-1}n_1-\ldots-rn_{L-1}}{n_L}. \qquad (10.3)$$

Даже тогда, когда заданы длины l_i кодовых слов и требуется, чтобы словарь был мгновенно декодируемым, он обычно продолжает оставаться недоопределенным и к нему могут быть предъявлены дополнительные требования.

Роль суммы $\sum_{i=1}^{N} r^{-l_i}$ становится более ясной после введения понятия *полного* словаря. Полным словарем называется такой словарь, что для любой полубесконечной последовательности символов найдется хотя бы одно кодовое слово, которое является префиксом этой последовательности. Как следствие этого, каждая конечная последовательность символов может быть интерпретирована как последовательность кодовых слов, оканчивающихся либо кодовым словом, либо префиксом кодового слова.

Теорема 10.3. Если словарь с N словами является полным, то $\sum_{i=1}^{N} r^{-l_i} \geqslant 1$, где l_i — длина i-го кодового слова.

Теорема 10.4. Любые два из свойств кодового словаря: 1) свойство полноты; 2) свойство префикса; 3) $\sum_{i=1}^{N} r^{-l_i} = 1$ влекут за собой третье.

Следствие. Если словарь является полным и декодируемым, то он обладает свойством префикса.

Следующие теоремы, относящиеся к полным словарям, будут полезны для дальнейших исследований.

Теорема 10.5. Если D — полный декодируемый словарь; p — префикс некоторого слова из D, а $D(p)$ — множество всех суффиксов s_i, таких, что ps_i является словом из D, то *суффиксное множество* $D(p)$ также является полным декодируемым словарем.

Теорема 10.6. Если декодируемый словарь D, использующий r-символьный алфавит, имеет N слов и является полным, то число различных префиксов слов из D равно $(N-r)/(r-1)$.

Следствие. Самое длинное слово в полном декодируемом словаре D с N словами имеет длину $L \leqslant (N-1)/(r-1)$.

Следствие. Полный декодируемый словарь D с N словами существует только тогда, когда $N = r + \lambda(r-1)$ для некоторого неотрицательного целого числа λ.

10.3. Коды Хаффмана

В этом параграфе описан алгоритм построения мгновенно декодируемых словарей, который минимизирует (по всем таким словарям) среднее число символов, необходимое для кодирования сообщения, при условии, что каждый выход источника кодируется индивидуально независимо от предшествующих и последующих выходов. (Это, конечно, не исключает возможности предварительной обработки с целью уменьшения избыточности в выходах, как указывалось в § 10.1.)

При описании алгоритма кодирования удобно ввести понятие r-ичного *дерева* (рис. 10.1, $r=3$); каждый *узел* является началом для r *ребер*; каждое ребро, в свою очередь, заканчивается узлом. Эти узлы называются *непосредственными потомками* начального узла. Если некоторый узел может быть получен из другого узла по последовательности непосредственных потомков, то он называется *потомком* этого узла. Приняты следующие обозначения: первый узел никак не обозначается; его r непосредственных потомков обозначаются r символами алфавита. В общем случае, непосредственные потомки узла, обозначенного $\alpha_1\alpha_2\ldots\alpha_i$, в свою очередь, обозначаются $\alpha_1\alpha_2\ldots\alpha_i\beta$, где β принимает значения r различных символов алфавита. Ясно, что все l-последовательности из r-символьного алфавита представляются как узлы на дереве такого типа. Словарь определяется посредством отождествления некоторых из этих узлов с кодовыми словами и игнорированием остальных.

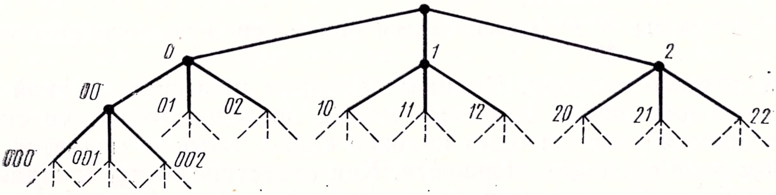


Рис. 10.1. Троичное дерево

Если словарь должен обладать свойством префикса, то никакой из потомков кодового слова не может быть, в свою очередь, кодовым словом. Если узел такого словаря является кодовым словом, то все узлы, являющиеся его потомками, должны быть выброшены из дерева; каждое кодовое слово при этом является *оконечным узлом*, которое не имеет потомков. Дерево такого типа называется *кодовым деревом*. Кодовое дерево, соответствующее словарю {0, 1, 20, 21, 220, 221, 222}, изображено на рис. 10.2. Так как все словари, которые могут быть представлены кодовым деревом, очевидно, являются мгновенно декодируемыми, то мы доказали следующую теорему.

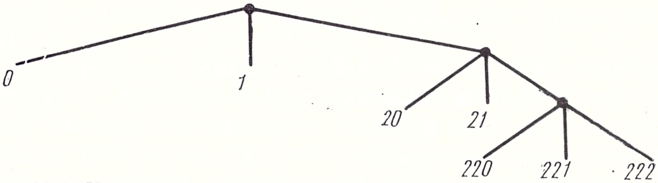


Рис. 10.2. Кодовое дерево

Теорема 10.7. Словарь является мгновенно декодируемым тогда и только тогда, когда он может быть представлен в виде кодового дерева.

Заметим, что некоторые из оконечных узлов дерева не обязательно будут принадлежать словарю, т. е. они могут соответствовать «символам источника», появляющимся с нулевой вероятностью.

Теорема 10.8. *Множество длин* $\{l_i\}$ *слов любого словаря, который может быть представлен в виде кодового дерева, удовлетворяет границе* (10.1) *со знаком равенства.* (Опять, для того чтобы усечь дерево, может оказаться необходимым включить некоторые кодовые слова, имеющие нулевую вероятность.)

Процедура построения мгновенно декодируемого словаря, который минимизирует среднее число кодовых символов, необходимых для кодирования символа источника, была предложена Хаффманом. Метод состоит в следующем. Пусть S_0 обозначает множество N символов источника, каждому из которых нужно поставить в соответствие некоторый узел кодового дерева. Возьмем r узлов, соответствующих r символам источника, имеющим наименьшую вероятность появления, и соединим их с помощью r ребер с одним и тем же составным узлом. Оставшиеся $N—r$ узлов вместе с составным узлом можно рассматривать как новый источник S_1, в котором составной узел представляет новый «символ», имеющий вероятность, равную сумме вероятностей соединенных с ним узлов. Аналогично соединим r наименее вероятных узлов источника S_1 с одним узлом и определим тем самым другой источник S_2 с $N—2(r—1)$ символами. Продолжим эту процедуру до тех пор, пока не останется лишь один узел. Это и определит кодовое дерево. Число рассматриваемых узлов уменьшается на $r—1$ на каждом шаге, поэтому на предпоследнем шаге останется в точности r узлов тогда и только тогда, когда

$$N = r + \lambda(r - 1), \tag{10.4}$$

где λ — некоторое целое число. (Отметим, что в таком виде можно представить число $N=r^\alpha$, где α — некоторое целое.) Если N не имеет такого вида, то следует ввести «фиктивные» символы источника, каждый из которых имеет нулевую вероятность, с тем, чтобы *а)*

Сообщения	Вероятности					
A_1	0,40	0,40	0,40	0,40	0,40	1,0
A_2	0,20	0,20	0,20	0,20	0,40	
A_3	0,10	0,10	0,12	0,18	0,20	
A_4	0,08	0,08	0,10	0,12		
A_5	0,05	0,08	0,10			
A_6	0,05	0,05	0,05			
A_7	0,05	0,05	0,05			
A_8	0,03	0,04				
A_9	0,02	0,03				
A_{10}	0,01					
A_{11}	0,01					

б)

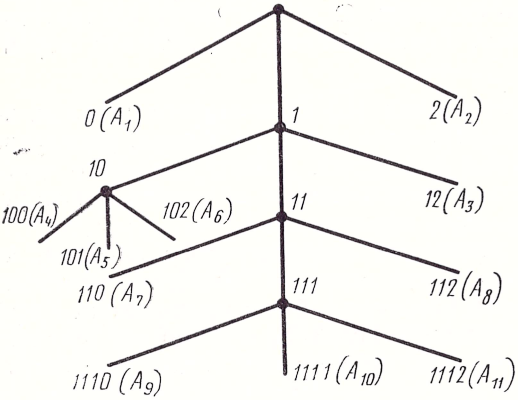


Рис. 10.3. Множество символов источника с их вероятностями *(а)* и дерево кода Хафмана для него *(б)* $(r=3)$

общее число символов, с учетом добавленных фиктивных символов, удовлетворяло равенству (10.4). Пример на рис. 10.3 помогает понять эту процедуру.

Кодовое дерево определяется алгоритмом Хафмана не однозначно. Так, например, на рис. 10.3*б* символы A_4, A_5 и A_6 могут быть, очевидно, переставлены, и это не повлияет на среднюю длину сообщения. Символы A_5, A_6 и A_7 также могли бы быть переставлены, так как вероятности каждого из них одинаковы.

Предположим, что символы источника S с N словами представляются словами или некоторым словарем D. Тогда средняя длина кодового слова определяется равенством

$$L = \sum_{i=1}^{N} p_i l_i, \tag{10.5}$$

где l_i — длина кодового слова, представляющего i-й символ источника, а p_i — вероятность того, что этот символ появится на выходе источника. Очевидно, что, по крайней мере, когда каждый символ источника кодируется независимо от предыдущих и последующих символов, среднее число символов, необходимых для представления последовательности символов источника, минимизируется при минимизации L. Чтобы словарь был однозначно декодируемым, множество длин кодовых слов $\{l_i\}$ должно удовлетворять границе (10.1).

Теорема 10.9. Никакой мгновенно декодируемый словарь не дает более короткую среднюю длину слова при представлении символов источника, чем соответствующий словарь Хаффмана.

Следствие. Никакой однозначно декодируемый словарь не дает более короткую среднюю длину слова, чем соответствующий словарь Хаффмана.

Алгоритм Хаффмана, таким образом, идеально подходит для ситуации, когда с помощью предварительной обработки зависимость между последовательными информационными символами была сведена к минимуму. В этом случае код Хаффмана использует каждый из r-ичных кодовых символов приближенно $(1/r)$-ю долю времени и каждой символ в закодированной последовательности дает минимум информации относительно следующего за ним символа. Это легко увидеть с помощью рассмотрения соответствующего кодового дерева. Каждый непосредственный потомок некоторого узла представляет событие, вероятность которого примерно равна вероятности событий, представляемых другими непосредственными потомками этого узла. Соответственно примерно равны вероятности появления любого символа вслед за любым другим, и любой символ используется приблизительно с одинаковой частотой.

10.4. Проверка произвольного словаря на однозначную декодируемость

Полезным средством при анализе свойства декодируемости какого-либо частного словаря является *суффиксное разложение* словаря. Суффиксное разложение словаря состоит в определении множеств S_i; эти множества определяются следующим образом. Множество S_0 представляет собой сам словарь, $S_0=D$. Множество S_i состоит из всех последовательностей символов s_i (которые называются *сегментами*), таких, что либо $s_{i-1}s_i=c$, либо $s_{i-1}=cs_i$, где c — некоторое слово из D, а s_{i-1} — какой-либо сегмент из S_{i-1}. Заметим, что каждый сегмент в каждом множестве S_i, $i\geqslant 1$ является суффиксом кодового слова. Для примера пусть $D=\{0, 10, 12, 21, 112, 1122\}$. Тогда суффиксное разложение D может быть записано в виде:

$$S_0=D=\{0, 10, 12, 21, 112, 1122\}, \quad S_1=\{2\}, \quad S_2=\{1\},$$
$$S_3=\{0, 2, 12, 122\}, \quad S_4=\{1, 2\}, \quad S_5=\{0, 2, 12, 122, 1\}\ldots$$

Причем все множества S_i совпадают при $i\geqslant 5$. Надо помнить, что имеются два критерия для включения последовательности символов в некоторое частное множество. Множество S_4, например, содержит элемент 1 потому, что 21 принадлежит D и 2 входит в S_3. Элемент 2 содержится в S_4, так как 12 принадлежит D, а 122 — S_3.

Укажем следующую теорему, связывающую свойство однозначной декодируемости с ограничением на суффиксное разложение D. Эта теорема впервые была доказана Сардинасом и Паттерсоном.

Теорема 10.10. Кодовый словарь является однозначно декодируемым тогда и только тогда, когда никакое кодовое слово не содержится ни в каком множестве S_i $(i \geqslant 1)$.

Чтобы более наглядно проиллюстрировать этот критерий, рассмотрим кодовый словарь $D=\{11, 010, 100, 110, 101, 0011\}$. Суффиксное разложение словаря начинается следующим образом:

$S_0=D$	S_1	S_2	S_3	S_4	S_5
11	0	10	0	10	0
010		011	1	011	1
100				1	00
110				00	10
101				01	01
0011					11

Как видим, множество S_5 содержит кодовое слово 11. Для того чтобы построить неоднозначно декодируемую последовательность, выберем $x_5=s_5=11$; $x_4=s_4=00$ (так что s_4s_5 — кодовое слово); $x_3=s_3=1$ $(s_3s_4=100)$; $x_2=s_2=10$ $(s_2s_3=101)$; $x_1=s_1=0$ $(s_1s_2=010)$ и $x_0=s_0=11$ $(s_0s_1=110)$. Последовательность $s_0s_1s_2s_3s_4s_5=1101010011$ может быть декодирована как 11, 010, 100, 11 и как 110, 101, 0011.

Пусть D^* обозначает словарь, получаемый обращением (считыванием справа налево) слов из словаря D (например, $D=\{1, 01, 02, 012\}$, тогда $D^*=\{1, 10, 20, 210\}$). Тогда справедлива

Теорема 10.11. Словарь D является однозначно декодируемым тогда и только тогда, когда словарь D^* однозначно декодируемый.

Пусть N_s обозначает число различных суффиксов слов из словаря D, которые сами не принадлежат D, и пусть N^*_s — соответствующее число для словаря D^*. При этом справедлива

Теорема 10.12. Чтобы определить, является ли данный словарь D декодируемым, необходимо исследовать не более n_0 множеств, включая множество $S_0=D$, где $n_0 \leqslant 1+\min[N_s, N^*_s]$.

В качестве примера рассмотрим кодовый словарь 10, 01, 011, 111. Суффиксами являются 0, 1, 11, так что $N_s=3$. Обращенный словарь 01, 10, 110, 111 имеет суффиксы 1, 0, 10, 11, так что $N^*_s=4$. Необходимо исследовать лишь четыре множества из таблицы. Так как ни одно из этих четырех множеств не содержит кодового слова, словарь является однозначно декодируемым. Фактически не было необходимости рассмат-

$S_0=D$	S_1	S_2	S_3	S_4
10	1	0	1	0
01		11	11	11
011				1
111				

ривать даже четвертое множество, все суффиксы появились в первых двух множествах. Кодовое слово, если бы оно вообще появилось, было бы замечено в одном из первых трех множеств. Или, что еще проще, ни одно из этих множеств не может содержать кодовое слово, так как в множествах S_i содержатся лишь суффиксы и так как никакой суффикс из D не является кодовым словом из D. Даже суффиксное разложение не было необходимым.

Интересно заметить, что, несмотря на то, что $N^*_s > N_s$, доказать однозначную декодируемость обращенного словаря D^* еще проще. Если $S_0 = D^*$, то множество S_1 пусто:

$S_0 = D^*$	S_1
01	
10	
110	
111	

Все остающиеся множества также пусты, и D^* (и, следовательно, D) является однозначно декодируемым словарем. Заметим, что D^* обладает свойством префикса и без дальнейших исследований ясно, что этот словарь является однозначно декодируемым. Все множества в суффиксном разложении какого-либо словаря, обладающего свойством префикса, будут, очевидно, пустыми, так как никакой суффикс не может в соединении с каким-либо кодовым словом дать другое кодовое слово. Обращение словаря, обладающего свойством префикса, дает словарь, обладающий свойством, которое можно назвать *свойством суффикса*: никакой суффикс кодового слова не является кодовым словом. Это следует либо из теоремы 10.11, либо из рассуждений предыдущего абзаца относительно того, что словарь, обладающий свойством суффикса, всегда однозначно декодируем.

Число различных суффиксов N_s кодовых слов из словаря D было использовано для того, чтобы получить границу числа множеств в суффиксном разложении словаря D, которые нужно рассмотреть, чтобы вынести суждение об однозначной декодируемости. Теперь используем это число N_s для других целей (например, для установления условия ограниченности задержки декодирования кодового словаря). Полезно получить верхнюю границу для N_s с помощью свойств самого словаря, не исследуя детально его суффиксов и не подсчитывая, сколько из них различных. Следующая теорема дает такую границу.

Теорема 10.13. Пусть D является словарем с N словами, составленными из r-символьного алфавита; обозначим через D_0 подмножество D, содержащее N_0 слов $(1 \leqslant N_0 \leqslant N)$ из D, которые не являются суффиксами каких-либо других слов из D. Тогда число N_s различных суффиксов из D, которые одновременно не являются словами D, ограничено неравенством

$$N_s \leqslant \sum_i i m_i - N_0 [\log_r N_0] + \frac{r}{r-1}\left(r^{[\log_r N_0]-1} - 1\right),$$

где m_i — число слов в D_0 длины i. Квадратные скобки обозначают целую часть величины, которая находится внутри них.

Используя суффиксное разложение кодового словаря, можно получить также необходимое и достаточное условие конечности задержки декодирования.

Теорема 10.14. Кодовый словарь D является декодируемым с конечной задержкой тогда и только тогда, когда множество S_{n_0} в суффиксном разложении D является пустым для некоторого $n_0 \leqslant N_s+1$.

Теорема 10.15. Если кодовый словарь является декодируемым с конечной задержкой d_c, то

$$\left[\frac{n_0}{2}\right] l_{\text{мин}} < d_c \leqslant \left[\frac{n_0+1}{2}\right] l_{\text{макс}},$$

где S_{n_0} — первое пустое множество в суффиксном разложении словаря, а $l_{\text{макс}}$ и $l_{\text{мин}}$ — числа символов в кодовых словах максимальной и минимальной длины соответственно.

Величина n_0 в теореме 10.15 ограничена сверху величиной N_s+1, а не минимумом из N_s+1 и N^*_s+1. В то время как обращение декодируемого кода декодируемо, обращение кода с конечной задержкой декодирования не обязательно имеет конечную задержку. Например, возьмем словарь $D=10$, 01, 011 и 111, который рассматривался ранее. Хотя как D, так и D^* декодируемы, последовательность 0110111011101110111... могла бы возникнуть как при передаче кодовых слов 01, 10, 111, 011, 10, 111, 011..., так и при передаче кодовых слов 011, 011, 10, 111, 011, 10, 111, 01. Для разрешения неоднозначности необходимо эту последовательность слов из D продолжить до бесконечности. Напротив, обращенный код D^* имеет задержку декодирования, равную трем, так как он обладает свойством префикса.

Глава 11

СИНХРОНИЗИРУЕМОСТЬ

11.1. Введение

Условие декодируемости для кодового словаря дает возможность разбить любую последовательность слов из словаря однозначно на отдельные слова, составляющие эту последовательность, *при условии, что задан начальный символ последовательности.* Во многих применениях, однако, начальный символ может не быть известен; например, возможно, что была начата передача сообщения до того, как приемник начинает свой прием, или возникшие ранее ошибки привели к неправильному декодированию первоначальной части сообщения. Если такая ситуация возникла, может оказаться необходимым, чтобы словарь был не только декодируемым, но и *синхронизируемым.* Последовательность слов, начинающаяся с кодового суффикса, называется *синхронизируемой с задержкой* d_s, если для однозначного определения начального символа, по крайней мере, одного из ее слов нужно знать не более d_s символов. Говорят, что словарь является синхронизируемым с задержкой d_s, если он декодируем и если каждая последовательность символов, составленная из слов этого словаря, синхронизируема с задержкой d_s или меньшей. Если термин «синхронизируемость» будет использоваться без какой-либо оговорки, то будет подразумеваться синхронизируемость с конечной задержкой.

Эта глава начинается с описания некоторых общих свойств, которыми должен обладать словарь, для того чтобы быть синхронизируемым. В следующем параграфе введено понятие *самосинхронизируемости* и исследованы некоторые свойства словаря, связанные с этим понятием[1]). В § 11.3 дана верхняя граница для числа слов различной длины, которые могут входить в какой-либо синхронизируемый словарь. Наконец, в § 11.5 описана конструкция, используя которую, всегда можно достичь этой границы.

11.2. Проверка словаря на синхронизируемость

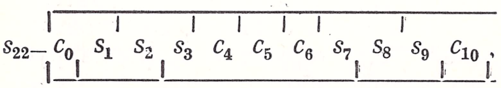
Требование, чтобы словарь был синхронизируемым, накладывает на любую принимаемую последовательность кодовых слов одно из следующих двух ограничений. Каждая последовательность символов, получаемая из последовательности слов с помощью отбрасывания, по крайней мере, одного начального символа (но не бо́льшего числа, чем в полном слове), является либо недекодируемой, либо декодируемой, но такой, что правильная синхронизация автоматически устанавливается после того, как первые несколько слов декодированы. Примером словаря, удовлетворяющего обоим условиям, является словарь, который состоит из слов $w_1=01$; $w_2=100$; $w_3=101$; $w_4=1101$. Если, например, первые два символа последовательности, начинающейся с $w_2w_4w_i\ldots$, не могут быть использованы при декодировании, то выходом декодера будет последовательность $w_1, w_3, w_i\ldots$ и синхронизм достигается ко времени приема w_i независимо от индекса i. Напротив, если в той же самой последовательности был опущен лишь первый символ, то декодер получит вначале символы 00. Так как никакое кодовое слово не начинается этим префиксом, то декодер опознает, что произошла синхронизационная ошибка и выберет в качестве начального какой-либо другой символ.

---

[1]) Представленные в § 11.2 методы разработаны В. И. Левенштейном. (*Прим. авт.*).

Теорема 11.1. Декодируемый словарь синхронизируем с конечной задержкой только тогда, когда он и его обращение декодируемы с конечной задержкой.

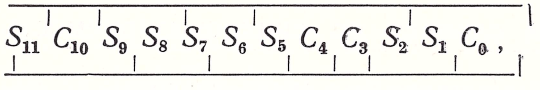
Доказательство. Предположим, что задержка декодирования для словаря D неограничена. Тогда существует некоторая последовательность с неограниченной длиной, которая не может быть декодирована однозначно. В обозначениях § 10.4, где c_i — слово, а s_i — кодовый суффикс в D, типичная недекодируемая последовательность имеет вид



$$s_{22}-c_0\ s_1\ s_2\ s_3\ c_4\ c_5\ c_6\ s_7\ s_8\ s_9\ c_{10}, \tag{11.1}$$

где отметки указывают два возможных варианта декодирования. Предположим, что нижние отметки соответствуют переданным кодовым словам. Тогда отбрасывание из префикса этой последовательности символов, составляющих $c_1=c_0s_1$, приводит к последовательности декодируемой с неограниченной задержкой, несмотря на то, что синхронизация ошибочна.

Аналогично предположим, что обращенный словарь D^* не декодируем с конечной задержкой. Тогда опять в обозначениях § 10.4 существует некоторая недекодируемая последовательность



$$S_{11}\ C_{10}\ S_9\ S_8\ S_7\ S_6\ S_5\ C_4\ C_3\ S_2\ S_1\ C_0, \tag{11.2}$$

которая теперь читается справа налево. (Здесь c_i и $s_i\ldots s_k$ — слова первоначального кода D. При считывании справа налево они являются словами обращенного кода. Аналогично все s_i, если читать справа налево, являются суффиксами и, так как задержка декодирования не ограничена, префиксами в D^*. Если их читать слева направо, то они, следовательно, будут как суффиксами, так и префиксами в D.) Так как s_{11}, например, является суффиксом кодового слова из D, то последовательность (11.2), читаемая слева направо, могла бы оказаться последовательностью слов из D с отброшенными начальными символами. Отметки под последовательностью соответствовали бы декодируемым словам, а верхние отметки — переданным словам. Синхронизация не будет достигнута до тех пор, пока не будет принято c_1. Но если задержка декодирования обращенного кода D^* не ограничена, то последовательность (11.2) может быть произвольно большой. Таким образом, в этом случае синхронизационная задержка словаря D также не ограничена ■ (здесь и далее ■ — конец доказательства).

В параграфе 10.4 было определено суффиксное разложение словаря D. Пусть S — множество суффиксов D; рассмотрим *суффиксное разложение множества* S, получаемое при использовании S, а не D в качестве S_0 — первого множества разложения. Вновь используя обозначения § 10.4, отметим, что любая декодируемая последовательность слов, начинающаяся с суффикса, может быть записана в виде

$$s_0x_1x_2x_3x_4 \cdot \cdot \cdot, \qquad (11.3)$$

где, как и ранее, x_i обозначает либо кодовое слово c_i, либо суффикс слова s_i. Снова любая подпоследовательность этой последовательности вида $s_ic_{i+1}c_{i+2}\ldots c_{i+j-1}s_{i+j}$ является кодовым словом. Более того, если ни одно из первых m множеств суффиксного разложения не является пустым, то последовательность вида (11.3) существует и содержит m элементов.

Теорема 11.2. Декодируемый словарь D является синхронизируемым тогда и только тогда, когда некоторое множество S_{n_0} в суффиксном разложении множества S суффиксов D является пустым при некотором целом $n_0 \leqslant \min(N_s, N^*_s)+1$. Величины N_s и N^*_s обозначают числа таких различных суффиксов, которые одновременно не являются кодовыми словами в словарях D и D^* соответственно.

Доказательство. Рассмотрим цепочку¹) сегментов из суффиксного разложения множества суффиксов S. Очевидно, что все последовательности кодовых слов, которые могут быть декодированы после того, как некоторые начальные символы были отброшены, характеризуются какой-либо такой цепочкой. Если словарь является синхронизируемым, то для всех этих последовательностей должна всегда иметь место одна из следующих двух ситуаций, описанных выше: либо в процессе декодирования должно быть достигнуто место, после которого невозможно произвести дальнейшее декодирование, либо декодирование должно войти в синхронизм и привести к правильному кодовому слову. Первые из этих ситуаций соответствуют условию, в котором некоторый сегмент из цепочки не является элементом следующего множества. Если имеет место второй случай, то слово, которое должно в конечном счете быть декодировано, является либо суффиксом переданного кодового слова, составляющего эту часть последовательности, либо имеет в качестве суффикса это переданное кодовое слово. В любом случае

---

¹) Ср. с § 10.4. *(Прим. авт.)*.

соответствующий сегмент из суффиксного разложения будет кодовым словом. Но по теореме 11.1, если словарь является синхронизируемым с конечной задержкой, то он также должен быть декодируем с конечной задержкой. Таким образом, когда сегмент является кодовым словом, цепочка, следующая за этим сегментом, должна по теореме 10.14 иметь конечную длину. Следовательно, все цепочки должны иметь конечную длину, и некоторое множество должно быть пустым для того, чтобы словарь был синхронизируемым. И, наоборот, если некоторое множество пусто, то все цепочки имеют конечную длину и либо невозможно декодировать соответствующую последовательность дальше при заданной начальной точке, либо декодирование должно войти в синхронизм с переданной последовательностью слов.

Чтобы оценить число сегментов, которые могут появиться в цепочке ограниченной длины, заметим снова, что ни одна из них не должна содержать повторяющихся сегментов. Так как множество S_0 содержит суффикс, то самое большее N_s—1 оставшихся суффиксов может быть включено в какую-либо цепочку. Учитывая второй режим достижения синхронизма, можно сказать, что один из этих сегментов может быть кодовым словом, а не суффиксом, но в силу того, что словарь является декодируемым, лишь один сегмент в цепочке может содержать слово. В соответствии с этим самая длинная цепочка может содержать самое большее N_s+1 сегментов, и множество S_{n_0} должно быть пустым для некоторого целого $n_0 \leqslant N_s+1$.

Предположим теперь, что существует некоторая цепочка, содержащая больше, чем N^*_s+1 сегментов. Эта цепочка при чтении справа налево соответствует некоторой цепочке в суффиксном разложении суффиксного множества словаря D^*. Так как D^* декодируем, то эта цепочка может также содержать самое большее одно кодовое слово в качестве сегмента. Если она содержит более чем N^*_s+1 сегментов, то некоторый суффикс D^* должен быть повторен и может быть построена бесконечная цепочка. Следовательно, $n_0 \leqslant N^*_s+1$, и теорема доказана ■.

В качестве примера рассмотрим словарь D_1 из слов {01, 101, 110, 001}. Так как D_1 обладает свойством префикса, то он, очевидно, является декодируемым. Но суффиксное разложение суффиксного множества словаря D_1 имеет вид, показанный в таблице, и так как $S_2=S_1$, то все последующие множества будут совпадать с S_1. Словарь не является синхронизируемым. В частности, последовательность

D_1	$S_0=S$	S_1	S_2
01	0	1	0
101	1	01	1
110	01	10	01
001	10		10

1 0 1 1 0 1 1 0 1 1 0 1

может быть бесконечно продолжена, причем невозможно установить правильную синхронизацию, если неизвестна начальная позиция.

В противоположность этому словарь $D_2=\{101,\ 00110,\ 10111,\ 11001\}$, который, как доказано в § 10.1, является декодируемым, является также и синхронизируемым в силу того, что

D_2	$S_0=S$	S_1	S_2	S_3	S_4
101	0	1	1	1	01
00110	1	01	01	01	0111
10111	01	10	10	111	1001
11001	10	001	111	0111	
	11	0110	0111	1001	
	001	0111	1001		
	110	1001			
	111	111			
	0110				
	0111				
	1001				

и S_5 пусто.

Теорема 11.3. Если словарь D является синхронизируемым, то задержка синхронизации d_s ограничена неравенством

$$\max\left\{d_c-l_{\text{макс}},\ d_c^*-l_{\text{макс}},\left[\frac{n_0-1}{2}\right]l_{\text{мин}}\right\}+1\leqslant d_s\leqslant\left[\frac{n_0+1}{2}\right]l_{\text{макс}}-1, \tag{11.4}$$

где d_c и d^*_c — задержки декодирования словарей D и D^* соответственно; $l_{\text{макс}}$ и $l_{\text{мин}}$ — числа символов в кодовых словах D максимальной и минимальной длины и S_{n_0} —первое пустое множество в суффиксном разложении множества суффиксов D.

Доказательство. Вывод верхней границы аналогичен использованному в теореме 10.15, но слегка усложнен тем, что первые m символов $(0\leqslant m\leqslant l_{\text{макс}}-2)$ несинхронизируемой последовательности максимальной длины не обязательно содержатся в соответствующем суффиксном разложении множества суффиксов D. [Первое кодовое слово, которое принимается полностью, может начинаться $(m+1)$-м символом, второе — k-м при некотором k из интервала $m<k<l_{\text{макс}}$. Очевидно, что, если $k\geqslant l_{\text{макс}}$, то $(m+1)$-й символ однозначно восстанавливается как первый символ первого правильного кодового слова.] Как и ранее, если n_0 четное, то существует четное число непустых множеств в суффиксном разложении (от

S_0 до S_{n_0-1}), и длина самой длинной последовательности, соответствующей этим n_0 множествам, не превосходит $(n_0/2)l_{\text{макс}}$ символов. Так как суффиксу из S_0 могут предшествовать в действительности вплоть до $l_{\text{макс}}-2$ дополнительных символов, фактически не входящих в суффиксное разложение, то $d_s \leqslant (n_0/2)l_{\text{макс}}+l_{\text{макс}}-2$. Если n_0 нечетное, то длина последовательности максимальной длины, не содержащая суффиксы множества S_0, ограничена величиной $[(n_0-1)/2]l_{\text{макс}}$. Эта последовательность следует за суффиксом слова (по крайней мере, часть которого принадлежит S_0), который не может содержать больше $l_{\text{макс}}-1$ символов. Следовательно, если n_0 нечетное, $d_s \leqslant ((n_0+1)/2)\,l_{\text{макс}}-1$, и теорема о верхней границе доказана.

Если словарь имеет задержку декодирования d_c, то существует последовательность длины d_c-1 вида (11.1), где ни один из двух возможных вариантов декодирования не может быть отброшен до тех пор, пока не будет принят d_c-й символ. Отбрасывание c_0 из префикса этой последовательности приводит к последовательности длины $d_c-1-(l_{\text{макс}}-1)$ (или большей длины), которая не является синхронизируемой. (В c_0 могут входить самое большее $l_{\text{макс}}-1$ символов, так как c_0s_1 является кодовым словом. Если бы не было отброшено все слово c_0, то можно было бы заключить на основе оставшегося суффикса, что в действительности было принято c_0. И так как оба варианта декодирования этой последовательности начинаются с первого символа c_0, то в этом случае не было бы синхронизационной неоднозначности.) Аналогично, если обращенный словарь имеет синхронизационную задержку d^*_c, то существует последовательность длины d^*_c-1 вида (11.2), для которой еще не устранена неоднозначность декодирования. Та же самая последовательность, читаемая слева направо, является последовательностью из D, начинающейся суффиксом слова из D и имеющей длину, по меньшей мере, равную $d^*_c-1-(l_{\text{макс}}-1)$, и не являющейся синхронизируемой. Как и ранее, величина $l_{\text{макс}}-1$ должна быть вычтена, так как по предположению можно завершить последовательность после получения первого символа из c_0. Наконец, рассуждения, приводящие к нижней границе в теореме 10.15, могут быть использованы здесь для того, чтобы показать, что $d_s \geqslant [(n_0-1)/2]l_{\text{мин}}$. Это завершает вывод нижней границы ■.

11.3. Самосинхронизирующиеся кодовые словари

Мы рассмотрели два механизма, посредством которых можно осуществлять синхронизацию. Один из этих механизмов работает, когда принимаемая последовательность недекодируема после определенного места: в этом случае обнаруживается потеря синхронизации (в предположении, что ни один из символов не является ошибочным), и декодер должен начать декодирование последовательности вновь, начиная с другого начального символа. Эта процедура имеет то преимущество, что она обнаруживает синхронизационную ошибку. Слова, декодированные, пока эта ошибка не была обнаружена, можно отбросить, а принятая последовательность декодируется вновь после того, как установлена правильная синхронизация.

Было также отмечено, что в некоторых случаях синхронизм получается автоматически. Декодер начинает работу с ошибочной синхронизацией, но в процессе декодирования фактически входит в правильный синхронизм, никогда не достигая места, которое он не может декодировать. Синхронизационная ошибка никогда не обнаруживается, и поэтому не делается попытка исправить неправильно декодированные до установления синхронизации слова. Тем не менее этот метод синхронизации имеет важное преимущество, состоящее в том, что он не приводит к дополнительному усложнению аппаратуры. Декодер достигает синхронизма без какого-либо видоизменения.

Последовательности, которые имеют то свойство, что декодер автоматически входит в правильный синхронизм даже тогда, когда начальные символы составляют суффикс слова, а не само кодовое слово, будут называться *самосинхронизирующимися* последовательностями. Если любую последовательность слов из декодируемого словаря D, начинающуюся с какого-либо суффикса какого-либо слова из D, можно сделать самосинхронизирующейся последовательностью, присоединив к ней в конце последовательность конечной длины, состоящую из слов, то D называется *абсолютно самосинхронизирующимся словарем.* Если некоторые или никакие из этих последовательностей не могут быть сделаны самосинхронизирующимися, то словарь называется соответственно *частично самосинхронизирующимся словарем* или *никогда самонесинхронизирующимся словарем.* Здесь не накладывается никаких ограничений на время до возникновения самосинхронизации; такие коды могут быть, а могут и не быть синхронизируемыми с конечной задержкой. Однако даже в случае, когда задержка является потенциально бесконечной, вероятность того, что бесконечная последовательность слов, выбираемых случайно из самосинхронизирующегося словаря, в конечном счете не войдет в синхронизм, равна нулю. Действительно, вероятность того, что на каком-либо этапе не будет выбрана обязательно синхронизирующая последовательность, меньше единицы, так что это событие может произойти бесконечное число раз только с вероятностью ноль.

Часто желательно, чтобы словарь был либо абсолютно самосинхронизирующимся, либо никогда самонесинхронизирующимся в зависимости от того, является ли простота процедуры декодирования более или менее важной по сравнению со способностью обнаруживать момент, когда происходит ошибка синхронизации. Частично самосинхронизирующийся словарь, в силу того что он должен производить синхронизацию при отсутствии самосинхронизирующейся последовательности, не обеспечивает ни снижения сложности декодера, ни гарантирует обнаружения всех ошибок синхронизации.

Теорема 11.4. Словарь D будет никогда самонесинхронизирующимся в том и только в том случае, когда никакие суффиксы D не являются одновременно кодовыми словами D.

Доказательство. Если имеется такая самосинхронизирующаяся последовательность, как, например, (в обозначениях § 10.4) последовательность

$$s_{-1}\quad s_{-2}\quad c_{-3}\quad s_{-4}\quad s_{-5}\quad s_{-6}\quad , \qquad (11.5)$$

в которой верхние отметки (представляющие декодированные слова в присутствии ошибок синхронизации) и нижние отметки (отмечающие переданные кодовые слова) будут находиться в фазе после получения суффикса s_6, то суффикс s_6 сам должен быть кодовым словом. Наоборот, всякий раз, когда суффикс s_0 в D является также некоторым кодовым словом c_0, последовательность s_0, получаемая отбрасыванием префикса из кодового слова с этим суффиксом, является самосинхронизирующейся. ■

Словарь D_1 из § 11.2 порождает некоторые самосинхронизирующиеся последовательности, поскольку все сегменты суффиксного разложения суффиксов словаря D_1 содержат слово 01. Очевидно, однословная последовательность 101 является самосинхронизирующейся при удалении первого символа, так как 01 также является кодовым словом. В противоположность этому словарь D_2 из того же самого параграфа согласно теореме 11.4 будет никогда самонесинхронизирующимся.

Абсолютно самосинхронизирующийся словарь D должен обладать следующими двумя свойствами:

1. Любая полубесконечная последовательность слов из D должна быть декодируемой в виде другой (возможно отличной) последовательности слов из D независимо от числа начальных символов, отброшенных в этой последовательности. Словарь, обладающий этим свойством, называется *разбиваемым*.

2. Должны существовать конечные *синхронизирующие последовательности*, состоящие из кодовых слов, которые способны обеспечить достижение синхронизма для любой из этих разбиваемых последовательностей. Это означает, что для каждой последовательности кодовых слов y, которой предшествует любой суффикс x любого кодового слова, должна существовать синхронизирующая последовательность z кодовых слов, такая, что последовательность xyz может быть полностью декодирована. (Так как z состоит только из кодовых слов и так как последовательность xyz должна оканчиваться словом, а не префиксом, то декодер должен достичь синхронизма, по крайней мере, ко времени, когда будет полностью декодирована последовательность xyz.)

Следующая теорема представляет собой прямое следствие второго из этих свойств.

Теорема 11.5. Если декодируемый словарь является абсолютно самосинхронизирующимся, то он должен обладать свойством префикса.

Доказательство. Предположим, что рассматриваемый словарь не обладает свойством префикса, так что p одновременно является кодовым словом и префиксом слова ps. Так как словарь является абсолютно самосинхронизирующимся, то должна существовать декодируемая последовательность sz, где z — последовательность кодовых слов. Но тогда декодирование последовательности psz возможно, по меньшей мере, двумя способами: в одном случае декодирование начинается кодовым словом p, во втором — кодовым словом ps. Следовательно, словарь не может быть одновременно самосинхронизирующимся и декодируемым, если он не обладает свойством префикса. ■

Разбиваемость, которой требует абсолютная самосинхронизируемость словаря, очевидно, имеет место, когда словарь полный, но, к сожалению, нужно иметь в виду некоторые другие соображения.

Теорема 11.6. Синхронизационная задержка декодируемых полных словарей является бесконечной, кроме случая, когда все слова содержат только один символ.

Доказательство. Если некоторое слово из словаря содержит более одного символа, то имеется, по крайней мере, один символ (назовем его a), который не является кодовым словом. Это утверждение является следствием того, что словарь должен обладать свойством префикса (теорема 10.4). Тогда последовательность $aaa\ldots$ представляет собой последовательность кодовых слов длины два или больше, так как словарь является полным, а символ a не является кодовым словом. Но эта последовательность, очевидно, не синхронизуемая. Если отбросить первый символ, то последовательность останется той же самой; не существует способа определения первого символа любого слова этой последовательности.

В силу этого может быть полезным рассмотрение словарей, которые обладают свойством префикса и которые являются разбиваемыми, но не полными. Для того чтобы описать такие словари, удобно определить *пополнение* D' словаря D таким образом, чтобы объединение D и D' было полным декодируемым словарем. Если D обладает свойством префикса, но не является полным, то всегда можно добавить к нему слова так, чтобы получить словарь, который будет полным, но все еще будет обладать свойством префикса. Систематический метод выполнения этого построения состоит в выписывании всех L-последовательностей (где L — длина самого длинного слова из D) и определении тех, которые не имеют в качестве префиксов слова из D. Эти последние L-последовательности могут быть отнесены к множеству D'. Хотя такая конструкция приводит к неоднозначному определению D', она будет использована в последующем рассмотрении. Пусть далее S будет множеством суффиксов $\{s_i\}$ в D и пусть S_1 будет множеством элементов $\{x_i\}$, причем x_i принадлежит множеству S_1 тогда и только тогда, когда

$s_j x_i = c'$ для некоторой L-последовательности c' из D' и некоторого суффикса s_j из S.

Теорема 11.7. Словарь D, обладающий свойством префикса, будет разбиваемым тогда и только тогда, когда никакой элемент из множества S_1 не является префиксом в D и не допускает представления в виде последовательности слов из D, за которой следует, возможно, префикс из D.

Доказательство. Если условие теоремы нарушается, то существует, очевидно, некоторый суффикс некоторого слова из D, который в случае, когда за ним следует последовательность слов из D, дает последовательность слов, содержащую некоторое слово из D'. Так как словарь $D+D'$ обладает свойством префикса, то эта же последовательность не может быть декодирована в виде последовательности слов лишь из D и D не будет разбиваемым.

Обратно, предположим, что имеется некоторая последовательность слов из D (начинающаяся суффиксом из S), которая не является разбиваемой. Тогда первая недекодируемая часть этой последовательности должна начинаться словом из D'. Это может произойти, только если существует суффикс в S, за которым может следовать последовательность из нуля или более слов из D, оканчивающаяся, возможно, префиксом из D, что даст слово из D'. Такая последовательность была бы элементом из S_1 и имела бы вид, запрещенный условием теоремы. (Заметим, что никакой элемент из S не может сам быть словом из D', так как все последние имеют длину L, в то время как все первые имеют длину, меньшую, чем L.) Это доказывает теорему ■.

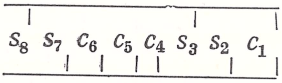
Для того чтобы показать, что множество разбиваемых, но неполных словарей не является пустым, рассмотрим словарь $D_1 = \{1, 01, 001, 0001\}$. Единственным словом, которое необходимо добавить для того, чтобы сделать множество полным, является 0000. Но, так как $S = \{1, 01, 001\}$, то S_1 является пустым, и D_1 является разбиваемым. В качестве второго, менее очевидного примера, рассмотрим словарь $D_2 = \{1, 001, 0001, 011, 0101, 01001, 010001\}$. Тогда $D' = \{000000, 000001, 000010, 000011, 010000\}$, $S = \{1, 01, 001, 11, 101, 1001, 0001, 10001\}$ и $S_1 = \{0000\}$. Поскольку никакая последовательность слов из D_2 не начинается с 0000, то D_2 разбиваемый.

До сих пор мы имели дело с первым из двух условий, необходимых для того, чтобы словарь был самосинхронизирующимся. Напомним, что второе условие требует существования синхронизирующей последовательности для каждой возможной последовательности слов, начинающейся суффиксом слова.

Для того чтобы облегчить рассмотрение необходимого и достаточного условия существования синхронизирующих последовательностей, введем *суффиксное множество* Q, определяемое как множество таких суффиксов некоторого словаря D, которые не являются словами из D и не имеют в качестве префиксов слова из D. Так, если $D = \{0, 100, 101, 110, 1110, 1111\}$, то $Q = \{1, 10, 11, 111\}$.

Теорема 11.8. Разбиваемый декодируемый словарь D является абсолютно самосинхронизирующимся тогда и только тогда, когда каждый из элементов обращения Q^* суффиксного множества Q содержится, по крайней мере, в одном множестве суффиксного разложения обращенного словаря D^*.

Доказательство. При заданном разложении D^* можно построить последовательность вида (ср. с § 10.4)



,

где последовательность читается справа налево. Отметки отделяют подпоследовательности, которые являются словами из D^*, а при чтении слева направо словами из D. В этом частном примере s_8 является суффиксом из D и верхние отметки отмечают декодирование, начинающееся с s_8, которое приводит к синхронизму, когда принимается слово c_1, что указано с помощью нижних отметок. Если такая последовательность существует, то существует, очевидно, синхронизирующая последовательность для любой последовательности кодовых слов, которая, будучи декодирована асинхронно, оставляет в качестве суффикса элемент, отмеченный в данном случае через s_8. Так как Q содержит все возможные суффиксы из D, которые не могут быть частично декодированы сами по себе, то словарь абсолютно самосинхронизирующийся, если каждый элемент Q^* содержится в некотором сегменте разложения D^*.

Обратно, если имеется некоторая синхронизирующая последовательность для некоторого суффикса из Q, то можно разложить ее на сегменты так, как это было сделано выше в частном примере. Эти сегменты, читаемые справа налево, определяют элементы последовательных множеств суффиксного разложения обращенного словаря D^*. Рассматриваемый суффикс должен содержаться в некотором множестве этого разложения, так что условие, указанное в теореме, является как необходимым, так и достаточным. ■

Рассмотрим опять словарь $D_1=\{1,\ 01,\ 001,\ 0001\}$. Здесь Q является пустым, так что условие теоремы 11.8 тривиально. Очевидно, что поскольку каждый суффикс является кодовым словом, словарь является абсолютно самосинхронизирующимся и в действительности является синхронизируемым с минимальной задержкой.

Вторым из рассмотренных разбиваемых словарей является словарь $D_2=\{1,\ 001,\ 0001,\ 011,\ 0101,\ 01001,\ 010001\}$, для которого $Q=\{01\}$, $Q^*=\{10\}$, а первые два множества в разложении D^*_2

$$S_0=D^*_2=\{1,\ 100,\ 1000,\ 110,\ 1010,\ 10010,\ 100010\};$$
$$S_1=\{0,\ 00,\ 000,\ 10,\ 010,\ 0010,\ 00010\}.$$

Так как S_1 содержит единственный элемент Q^*, то этот словарь также является абсолютно самосинхронизирующимся.

В противоположность этому словарь $D_3=\{11,\ 00,\ 01,\ 1000,\ 1001,\ 1010,\ 1011\}$ является полным и декодируемым. Но $Q=\{0,\ 1,\ 10\}$;

$Q^*=\{0, 1, 01\}$, и разложение D^*_3 имеет вид $S_0=D^*_3=\{11, 00, 10, 0001, 1001, 0101, 1101\}$; $S_1=\{01\}$; $S_2=\{01\}$; $S_3=\{01\}$. Все последующие множества содержат лишь 01, так что D_3 не является абсолютно самосинхронизирующимся словарем. В частности, никакая последовательность слов не может быть присоединена к какой-либо последовательности, начинающейся с суффикса, имеющего нечетную длину, для того чтобы сделать ее самосинхронизирующейся, так как все последовательности слов имеют четную длину и любая последовательность начинающаяся суффиксом, имеющим нечетную длину, за которым следуют кодовые слова из D_3, будет иметь нечетную длину. Это рассуждение можно, очевидно, обобщить и сформулировать следующую теорему.

Теорема 11.9. Любой словарь, имеющий слова с длинами, общим делителем которых является некоторое целое число b, большее единицы, не может быть абсолютно самосинхронизирующимся. (Заметим, в частности, что это относится ко всем словарям, имеющим одинаковые длины слов $b>1$.)

Поскольку множество P всех префиксов слов словаря, по-видимому, более удобно для использования, чем множество Q, то полезной оказывается следующая теорема.

Теорема 11.10. Если множество Q в формулировке теоремы 11.8 заменить на P (множество префиксов словаря D), то теорема остается справедливой.

Доказательство. Ясно, что для того, чтобы словарь был разбиваемым, все элементы Q должны содержаться в P. Условие теоремы 11.8 при замене Q на P, конечно, будет достаточным. Для того чтобы доказать необходимость этого условия при замене Q на P, покажем, что каждый элемент P^* должен содержаться в некотором множестве суффиксного разложения D^*, если это утверждение справедливо для каждого элемента Q^*. Это следует сразу же в силу того, что любой элемент p^* из P^* может быть использован для построения слова, имеющего либо вид $w^*_1=w^*_2w^*_3...w^*_lp^*$, либо вид $w^*_1=q^*w^*_2w^*_3...w^*_lp^*$, где w^*_i — слова из D^*, а q^* принадлежат Q^*. Поскольку в каждом из этих двух случаев все слова из D^* содержатся в множестве S_0 и все элементы Q^* содержатся в некотором множестве, то же должно быть верным для всех элементов P^*. ■

Оценим теперь число множеств суффиксного разложения D^*, которое нужно исследовать для того, чтобы узнать, можно ли словарь D классифицировать как абсолютно самосинхронизирующийся.

Теорема 11.11. Если разбиваемый декодируемый словарь D является абсолютно самосинхронизирующимся, то требуется проверить не более n_1 множеств суффиксного разложения D^*, чтобы установить, выполняются ли условия теоремы 11.8, где $n_1 \leqslant N_p$ и где N_p — число префиксов из D.

Доказательство. Прежде всего, заметим, что $N_p = N^*_s$, т. е. число префиксов D равно числу суффиксов D^*. Доказательство после этого становится аналогичным доказательству теоремы 11.2. Каждая запись элемента в некоторое множество зависит только от элементов предыдущего множества. Поэтому после некоторого множества, содержащего только элементы, которые уже появлялись в предыдущих множествах, никаких новых элементов в разложении не появится. Необходимо лишь выяснить, как долго будут появляться новые сегменты в каждом множестве. Так как существует лишь $N^*_s = N_p$ возможных сегментов, теорема доказана. ■

Наиболее простые разбиваемые словари — это полные словари. Основной недостаток этого класса словарей состоит в их неограниченной синхронизационной задержке (теорема 11.6). Этот недостаток можно преодолеть, однако, используя *универсальную синхронизирующую последовательность.* Универсальной синхронизирующей последовательностью называется последовательность, которая эффективно декодируется независимо от предшествующего ей суффикса. Если периодически вставлять такую последовательность в поток кодовых слов, то можно быть уверенным, что декодер будет в синхронизме после декодирования этой последовательности, даже если до этого он не был в синхронизме. При этом, конечно, вносится избыточность в систему, но то же самое происходит и при всех других методах синхронизации, рассматриваемых в этой главе. Другие рассматриваемые методы используют более сильные ограничения на число слов в словаре по сравнению с тем ограничением, которое наложено условием декодируемости. Метод универсальной синхронизирующей последовательности позволяет использовать полностью декодируемый словарь, но при этом необходимо периодически включать кодовые слова, не переносящие информацию. Покажем теперь, что такие последовательности существуют.

Теорема 11.12. Для любого абсолютно самосинхронизирующегося словаря существует универсальная синхронизирующая последовательность.

Доказательство. Так как словарь является абсолютно самосинхронизирующимся, то для каждого суффикса s существует последовательность кодовых слов σ, такая, что любая последовательность кодовых слов после приема последовательности $s\sigma$ будет декодирована синхронно. Построим универсальную синхронизирующую последовательность следующим образом. Пусть w_L — одно из кодовых слов максимальной длины L. Оно будет первым словом в синхронизирующей последовательности. Любая несинхронно декодируемая последовательность, за которой следует слово w_L, будет давать в остатке один из $L-1$ возможных суффиксов этого слова. Если последнее декодированное слово было словом w_L или суффиксом w_L, то синхронизм уже достигнут. Предположим поэтому, что остаток после последнего декодированного слова является таким суффиксом s_1 слова w_L, который не является кодовым словом. Тогда должна существовать синхронизирующая последовательность σ_1 для этого суффикса s_1. Предположим вместо этого, что остается суффикс s_2. Обозначим тогда через s'_2 суффикс, остающийся после декодирования сегмента $s_2\sigma_1$, и присоединим синхронизирующую последовательность σ_2 этого суффикса к универсальной синхронизирующей последовательности, которую мы строим. В общем случае суффикс s_i приводит после декодирования последовательности $s_i\sigma_1\sigma_2...\sigma_{i-1}$ к суффиксу s'_i, для которого, в свою очередь, синхронизм достигается с помощью последовательности слов σ_i. Поступая таким образом, можно построить универсальную синхронизирующую последовательность вида $\Sigma = w_L\sigma_1\sigma_2\sigma_3...\sigma_{L-1}$, так что, если суффикс s_i слова w_L остается, когда декодер впервые сталкивается с этой последовательностью, то синхронизм будет достигнут ко времени, когда будет получена подпоследовательность σ_i, и, конечно, синхронизм сохранится во время декодирования оставшейся части синхронизирующей последовательности Σ. ■

Рассмотрим в качестве примера полный словарь $D = \{00, 111, 1100, 1101, 1000, 1001, 1010, 1011, 0100, 0101, 0110, 0111\}$.

Имеем

$D = \{00, 111, 1100, 1101, 1000, 1001, 1010, 1011, 0100, 0101, 0110, 0111\}$;

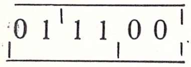
$P = Q = \{0, 1, 11, 100, 01, 101, 10, 010, 011, 110\}$;

$S_0 = D^* = \{00, 111, 0011, 1011, 0001, 1001, 0101, 1101, 0010, 1010, 0110, 1110\}$;

$S_1 = \{11, 01, 10, 0\}$;

$S_2 = \{1, 01, 10, 11, 0, 011, 001, 101, 010, 110\}$.

Поскольку множество P^* содержится в S_2, то словарь является абсолютно самосинхронизирующимся. Универсальная синхронизирующая последовательность может начаться, например, с четырехсимвольного слова $w_L = 0111$. Тогда, если суффикс, остающийся после декодирования последнего слова, предшествующего этой последовательности, равен $s_1 = 111$, то синхронизм уже достигнут. Если суффиксом будет $s_2 = 11$, то синхронизирующая последовательность для него будет состоять из одного слова 00, т. е.



,

так что универсальная синхронизирующая последовательность приобретает вид 011100. Наконец, если остается суффикс $s_3 = 1$, то суффиксом s'_3 будет 100 и в качестве σ_3 можно выбрать слово 0111. Полная универсальная синхронизирующая последовательность при этом равна $\Sigma = 0111000111$. Другая последовательность могла бы быть построена, если начать с некоторого другого четырехсимвольного слова. Наиболее короткая универсальная синхронизирующая последовательность 1000111 получается, например, когда выбирается $w_L = 1000$.

Теорема 11.13. Каждый самосинхронизирующийся кодовый словарь имеет универсальную синхронизирующую последовательность длины не большей, чем λ, где $\lambda \leqslant \left[\frac{n_1+3}{2}\right] L(L-1)$ и где n_1 определяется так же, как в теореме 11.1; L — длина максимального кодового слова, а квадратные скобки обозначают целую часть стоящей в них дроби.

Доказательство. Для заданного разложения D^* можно так же, как и в доказательстве теоремы 11.8, построить синхронизирующую последовательность для любого суффикса из Q. Самая длинная из таких последовательностей будет содержать n_1 сегментов и кодовое слово в конце. Последовательность, построенная из этих сегментов (см. § 10.4), такова, что любые два смежных сегмента имеют длину не более L символов. Следовательно, длина любой такой последовательности не больше, чем $[(n_1/2)+1]L$, символов, если n_1 четное, и $[(n_1+3)/2]L$ символов, если n_1 нечетное. Согласно конструкции из теоремы 11.12 универсальная синхронизирующая последовательность состоит не более чем из $L-1$ таких последовательностей. Таким образом, теорема доказана. ■

Мы говорили, что обычно словари должны быть либо абсолютно самосинхронизирующимися, либо никогда самонесинхронизирующимися. Первые имеют то преимущество, что они не требуют какого-либо дополнительного оборудования для получения синхронизации. Часто, однако, здесь возникают трудности из-за возможной неограниченной задержки синхронизации. Как было показано в теореме 11.12, ее можно устранить с помощью периодической передачи универсальной синхронизирующей последовательности; такие последовательности существуют для всех абсолютно самосинхронизирующихся кодов. Кроме того, хотя все полные коды имеют недостаток (неограниченную задержку), не все самосинхронизирующиеся коды таковы. Любой словарь вида $D_n=\{1, 01, 001, 001, 00001...\}$ (содержащий все слова вида 00...01 вплоть до длины n), в котором все суффиксы также являются кодовыми словами, очевидно, является самосинхронизирующимся с конечной задержкой. В действительности эти коды можно было бы называть *мгновенно синхронизируемыми,* так как синхронизм получается автоматически после приема любого полного суффикса. Длины слов в этом частном словаре D_n таковы, что

$$\sum_{i=1}^{n} 2^{-l_i} = 1 - \frac{1}{2^n}.$$

Следовательно, D_n почти достигает верхней границы в неравенстве Крафта, определяющем свойство декодируемости. Ограничение на синхронизируемость не обязательно значительно увеличивает избыточность кода, по сравнению с той, которая требуется лишь для однозначной декодируемости. Вопрос о максимальном числе слов в синхронизируемом словаре рассматривается в следующем параграфе.

11.4. Верхняя граница для числа слов в синхронизируемом словаре

Пусть w обозначает n-последовательность, а w^i — обозначает n-последовательность, получаемую циклической перестановкой символов w на i позиций вправо. Таким образом, если $w = (\omega_0\omega_1...\omega_{n-1})$, то $w^i = (\omega_{n-i}\omega_{n-i+1}...\omega_{n-1}\omega_0...\ \omega_{n-i-1})$. Если $w_1 = w^i_2$ для некоторого целого i, то говорят, что w_1 и w_2 принадлежат одному и тому же *классу эквивалентности*. Максимальное число различных слов длины n в классе эквивалентности равно, очевидно, n, так как $w^n = w$ для любого слова w. Некоторые классы эквивалентности, которые называются *вырожденными,* содержат меньше, чем n слов. [Слово $w = (00...0)$, например, является единственным словом в своем классе эквивалентности.] Если w принадлежит вырожденному классу эквивалентности, то $w = w^i$ для некоторого целого i из интервала $1 \leqslant i \leqslant n-1$.

Если словарь синхронизируем (с конечной задержкой), то он, очевидно, не может содержать двух слов из одного и того же класса эквивалентности. Если не считать префикс, то последовательности слов $www...$ и $w^iw^iw^i...$ тождественны и не существует способа определения начального символа такой последовательности, если как w, так и w^i принадлежат словарю. Аналогично никакой синхронизируемый словарь не может содержать *никакого* слова из вырожденного класса эквивалентности. Если $w = w^i$, то бесконечная последовательность $www...$ не изменяется, когда первые i символов отбрасываются и не существует способа определить, какой символ является начальным символом кодового слова.

Таким образом, показана справедливость следующей леммы.

Лемма 11.1. Число n-символьных слов в любом синхронизируемом коде, составленном из r-символьного алфавита, ограничено величиной $N(n, r)$, где

$$N(n, r) = W(n, r)/n \tag{11.6}$$

и где $W(n, r)$ — число n-последовательностей, принадлежащих невырожденным классам эквивалентности.

Рассмотрим в качестве примера множество двоичных последовательностей длины 4. Классы эквивалентности, содержащие последовательности длины 4 0000 и 1111, имеют только по одному элементу, класс, содержащий последовательности длины 4 0101, 1010, содержит лишь эти два элемента. Оставшиеся $2^4-2-2=12$ 4-последовательностей принадлежат невырожденным классам эквивалентности. Следовательно, имеется точно $12/4=3$ таких классов, каждый из которых вносит самое большее одно слово в любой словарь, который будет синхронизируемым. Существование синхронизируемого словаря с тремя словами доказывается примером множества {0001, 0011, 0111}.

Если n-последовательность имеет то свойство, что $w = w^{\nu}$ для некоторого целого ν, то говорят, что она периодическая с периодом ν. Слово длины n принадлежит вырожденному классу эквивалентности тогда и только тогда, когда оно является периодическим с некоторым периодом $0<\nu<n$. Следующие две леммы будут полезны при определении числа слов $W(n, r)$ в невырожденных классах эквивалентности.

Лемма 11.2. Если последовательность w длины n является периодической с периодами $\nu_1, \nu_2, \ldots$ и если ν_1 наименьший из этих периодов, то

1. $\nu_1 | \nu_i$ для всех i (т. е. $\nu_i = l_i \nu_1$ для некоторого целого l_i);
2. $\nu_1 | n$.

Доказательство. Пусть $\nu_i = q_i \nu_1 + r_i$, где q_i — неотрицательное целое число, а r_i — целое число из интервала $0 \leqslant r_i < \nu_1$. Если w является периодической с периодами ν_i и ν_1, то $w = w^{\nu_i} = w^{q_i \nu_1 + r_i} = w^{r_i}$. Так как ν_1 является наименьшим целым i, для которого $w^i = w$, то отсюда следует, что $r_i \geqslant \nu_1$ или $r_i = 0$. Но так как r_i принадлежит интервалу $0 \leqslant r_i < \nu_1$, то $r_i = 0$ и $\nu_i = q_i \nu_1$ для некоторого целого q_i. Это справедливо для всех периодов ν_i последовательности w, в том числе для $\nu_i = n$. Лемма доказана. ■

Лемма 11.3. Пусть A — подмножество элементов множества S, имеющих свойства a; обозначим через $N(A)$ число элементов в A. Тогда число элементов в S, имеющих какое-либо из свойств $a_1, a_2, \ldots, a_m$ (т. е. число элементов в множестве $A_1 + A_2 + \ldots + A_m$), равно

$$N(A_1 + A_2 + \ldots + A_m) = \sum_i N(A_i) - \sum_i \sum_{j<i} N(A_i A_j) +$$

$$+ \sum_i \sum_{j<i} \sum_{k<j} N(A_i A_j A_k) - \ldots - (-1)^m N(A_1 A_2 \ldots A_m), \qquad (11.7)$$

где $N(A_i, A_j \ldots A_\nu)$ — число элементов, имеющих *все* свойства $a_i, a_j, \ldots, a_\nu$ (т. е. число элементов в множестве $A_i A_j \ldots A_\nu$).

Доказательство. Доказательство проводится индукцией по m. Очевидно, если $m=2$, то

$$N(A_1 + A_2) = N(A_1) + N(A_2) - N(A_1 A_2),$$

так как число элементов в $A_1 A_2$ включается как в $N(A_1)$, так и в $N(A_2)$ и, следовательно, подсчитывается дважды в сумме $N(A_1) + N(A_2)$. Предположим теперь, что лемма справедлива для некоторого $m \geqslant 2$. Тогда, положив $B = A_1 + A_2 + \ldots + A_m$, получим

$$N(A_{m+1} + B) = N(A_{m+1}) + N(B) - N(A_{m+1} B). \qquad (11.8)$$

Но так как B и $A_{m+1}B$ представляют собой сумму (объединение) m подмножеств, то как $N(B)$, так и $N(A_{m+1}B) = N(A_1 A_{m+1} + A_2 A_{m+1} + \ldots + A_m A_{m+1})$ удовлетворяют равенству (11.7) согласно предположению индукции. Объединяя (11.7) и (11.8), получаем выражение, эквивалентное (11.7), но содержащее $m+1$ подмножеств, и доказательство леммы следует из принципа индукции.

Теперь можно доказать следующую теорему.

Теорема 11.14. Число n-символьных слов из r-ичного алфавита в синхронизируемом коде не может быть больше, чем

$$N(n, r) = \frac{1}{n} \sum_{d \mid n} \mu(d)\, r^{n/d}, \tag{11.9}$$

где суммирование производится по всем целым d, которые являются делителями n и где[1])

$$\mu(d) = \begin{cases} 1 & \text{при } d = 1; \\ (-1)^k & \text{при } d = p_1 p_2 \ldots p_k \ (p_1, p_2, \ldots, p_k \text{—различные простые; числа}); \\ 0 & \text{в остальных случаях.} \end{cases}$$

Доказательство. Предположим, что w — вырожденная n-последовательность с минимальным периодом ν. Согласно лемме 11.2 период ν должен, очевидно, равняться n/d, где d — некоторый целый делитель n. Очевидно, что w также вырожденная последовательность с периодом l_ν где l — некоторое целое число. Так как любое целое d можно записать в виде произведения степеней простых чисел, то получаем, что $\nu = n/d < n$ является периодом w только тогда, когда $l_\nu = n/p$, где p — некоторый простой делитель n. Для того чтобы найти число $W_d(n, r)$ вырожденных n-последовательностей, необходимо, следовательно, лишь подсчитать число тех n-последовательностей, которые имеют какой-либо из периодов n/p_j, где $(p_1, p_2, \ldots, p_l)$ — множество простых делителей n. Но если w является n-последовательностью с периодом n/d, то она должна иметь вид $w = ss \ldots s$, где s — некоторая (n/d)-последовательность. Так как любая n-последовательность такого вида является периодической с периодом n/d, то существуют точно $r^{n/d}$ n-последовательностей, имеющих этот период. Таким образом, используя лемму 11.3 и замечая согласно лемме 11.2, что w будет вырожденной с периодами n/p_j для всех $j = j_1, j_2, \ldots, j_\mu$ тогда и только тогда, когда она также вырождена с периодом $n/p_{j_1} p_{j_2} \ldots p_{j_\mu}$, получаем

$$W_d(n, r) = \sum_i r^{n/p_i} - \sum_i \sum_{j<i} r^{n/p_i p_j} +$$

$$+ \sum_i \sum_{j<i} \sum_{k<j} r^{n/p_i p_j p_k} \ldots - (-1)^l r^{n/p_1 p_2 \ldots p_l}. \tag{11.10}$$

Поэтому число невырожденных n-последовательностей равно $W(n, r) = r^n - W_d(n, r)$; максимальное число n-последовательностей в синхронизируемом коде равно $1/n$-й этой величины (лемма 11.1). Теорема доказана.

Теорема 11.4 основана на том, что никакие два слова с одной и той же длиной в синхронизируемом коде не могут принадлежать к одному и тому же классу эквивалентности и что ни одно из слов не принадлежит вырожденному классу эквивалентности. В случае, когда словарь содержит слова неодинаковой длины, та же самая идея может быть использована, чтобы улучшить границу для числа слов в синхронизируемом коде. Предположим, что две различных последовательности слов оказались в одном и том же классе эквивалентности [например, предположим, что некоторую циклическую перестановку n-символьного слова можно было бы также получить, если поместить за k-символьным словом $(n-k)$-символьное слово; все три слова принадлежат одному и тому же словарю]. Если бы две последовательности S_1 и S_2, составленные из различных кодовых слов, были фактически тождественными, то код не мог бы даже быть однозначно декодируемым. Если бы они были связаны циклической перестановкой, то бесконечные последовательности $...S_1S_1S_1...$ и $...S_2S_2S_2...$ не могли бы быть различены без помощи какого-нибудь постороннего метода, используемого для определения начального символа, и код был бы несинхронизируемым.

---

[1]) Функция $\mu(d)$ называется μ-функцией Мебиуса. Она часто встречается в комбинаторных задачах. *(Прим. авт.).*

Для того чтобы сделать это условие более точным, определим класс эквивалентности *по словам*, в противоположность классу эквивалентности *по символам*, как множество всех последовательностей слов, которые отличаются лишь циклической перестановкой *слов* в последовательности. Так, например, если $w_1=0011$, $w_2=01$ и $w_3=10$, то последовательности символов $w_1=0011$ и $w_2w_3=0110$ принадлежат одному и тому же классу эквивалентности по символам. Однако последовательности слов w_1 и w_2w_3 не находятся в одном и том же классе эквивалентности по словам, так как одна из них не может быть получена с помощью циклической перестановки другой. В противоположность этому последовательности слов $w_1w_2w_3$; $w_3w_1w_2$ и $w_2w_3w_1$ все принадлежат одному и тому же классу эквивалентности по словам. Заметим, что символы, которые составляют слова, не играют роли в определении класса эквивалентности по словам.

Предыдущие рассуждения, относящиеся к требованию, чтобы различные последовательности слов принадлежали различным классам эквивалентности по символам, приводят к следующему выводу.

Лемма 11.4. Если словарь D является синхронизируемым, то число невырожденных классов эквивалентности слов из D, имеющих полную длину n, не может быть больше числа невырожденных классов эквивалентности последовательностей символов длины n при любом целом n.

Доказательство. Пусть S_1 и S_2 — две различные последовательности символов, соответствующие последовательностям слов W_1 и W_2 соответственно. Предположим далее, что S_1 и S_2 принадлежат одному и тому же классу эквивалентности по символам, но что W_1 и W_2 принадлежат двум различным классам эквивалентности по словам. Бесконечная последовательность $...S_1S_1...$ может быть интерпретирована либо как $...W_1W_1...$, либо как $...W_2W_2...$, в зависимости от того, какой символ принимается в качестве начального. Но

W_1 и W_2 не связаны циклической перестановкой. Следовательно, в отсутствие априорной синхронизации возможны два различных способа декодирования, и словарь не является синхронизируемым. Аналогично, если S_1 вырожденная последовательность, а W_1 — невырожденная, тогда либо S_1 неоднозначно декодируема, либо последовательность $...S_1S_1...$ может быть декодирована двумя различными способами, если начинать с различных символов. Синхронизируемость требует, таким образом, чтобы любые две последовательности слов из различных невырожденных классов эквивалентности по словам приводили к двум последовательностям символов, которые были в различных невырожденных классах эквивалентности по символам. Таким образом, лемма доказана. ■

Заметим, что до тех пор, пока не будут наложены ограничения на допустимые *последовательности* слов, так же как на сами слова, все циклические перестановки какой-либо последовательности слов, очевидно, будут возможными. Синхронизируемость более высокого порядка может привести к запрещению для использования всех, кроме одной, последовательностей слов из каждого класса эквивалентности по словам. Это означает, что второй уровень кодирования можно было бы установить для самих кодовых слов, чтобы, например, получить возможность определить синхронизацию кадров так же, как и синхронизацию слов непосредственно по последовательности символов.

Для того чтобы найти число классов эквивалентности слов, имеющих длину n символов, рассмотрим вначале число способов представления n в виде суммы положительных целых чисел (т. е. числа *упорядоченных разбиений* целого числа n). В качестве примера число 4 может быть записано в виде

$$4 = 1 + 1 + 1 + 1 = 1 + 1 + 2 = 1 + 2 + 1 = 2 + 1 + 1 = 2 + 2 =$$
$$= 1 + 3 = 3 + 1 = 4.$$

Назовем два разбиения n эквивалентными, если одно является циклической перестановкой другого. Множество разбиений, состоящих из одного представителя из каждого класса эквивалентности, называется множеством *полуупорядоченных разбиений* S числа n. Полуупорядоченные разбиения числа 4, в частности, могут быть представлены последовательностями 1111, 112, 22, 13, 4.

Разбиение S числа n является последовательностью целых чисел. Пусть ν — минимальный период этой последовательности S, обозначим через P первые ν целых чисел из S и через $s(P)$ — единственное целое число, такое, что $S = PP \ldots P = P^{s(P)}$, где последовательность P повторяется $s(P)$ раз. Таким образом, когда $n=4$, имеем (см. табл.).

S	P	$s(P)$
1111	1	4
112	112	1
22	2	2
13	13	1
4	4	1

Предположим теперь, что синхронизируемый словарь D содержит σ_i слов длины i и пусть $S=ij...kij...k...k=P^{s(P)}$ — разбиение n.

Лемма 11.5. Число различных невырожденных классов эквивалентности, представленных словами синхронизируемого словаря D, имеющими соответствующие длины, представляемые разложением $S=P^{s(P)}$ числа n, равно

$$N[s(P),\ \sigma_i\sigma_j\ldots\sigma_k], \tag{11.11}$$

где $N(n, r)$ определено ф-лой (11.9).

Доказательство. Имеются $\rho=\sigma_i\sigma_j...\sigma_k$ множеств слов D, соответствующих последовательности $ij...k$. Рассматривая каждое из этих множеств как один символ нового алфавита, можем рассмотреть первоначальную последовательность слов как последовательность $s(P)$ этих новых «символов». Очевидно, что имеются $N[s(P), \rho]$ невырожденных классов эквивалентности, представленных «словами» этого вида, что и требовалось доказать. ■

С помощью этого результата легко доказать следующую теорему.

Теорема 11.15. Если D является синхронизируемым словарем, имеющим σ_i слов длины i, то

$$\sum_S N[s(P),\ \sigma_i\sigma_j\ldots\sigma_k] \leqslant N(n, r),\ n=1, 2,\ldots, \tag{11.12}$$

где суммирование проводится по всем полуупорядоченным разбиениям $S=P^{s(P)}$ числа n и где $P=ij...k$.

Доказательство. Согласно лемме 11.4 число эквивалентных классов последовательностей символов какой-либо длины n должно быть, по крайней мере, таким же, как число эквивалентных классов последовательностей слов этой длины. Но для каждого разбиения S существуют $N[s(P), \sigma_i\sigma_j...\sigma_k]$ классов эквивалентности по словам, представленных с помощью слов из D (лемма 11.5). Очевидно, что последовательности слов, соответствующие различным разбиениям, должны принадлежать различным классам эквивалентности. Общее число классов эквивалентности по словам при любом заданном n поэтому задается суммой, стоящей в левой части неравенства (11.12). Число классов эквивалентности по символам этой длины равно просто $N(n, r)$, что и доказывает справедливость неравенства (11.12), которое должно удовлетворяться для всех целых n. ■

Приведем пример: при $n=4$, $r=2$ имеем

$$\sum_S N[s(P), \sigma_i\sigma_j\ldots\sigma_k] = N(4,\ \sigma_1) + N\left(1,\ \sigma_1^2\sigma_2\right) +$$

$$+ N(2, \sigma_2) + N(1, \sigma_1\sigma_3) + N(1, \sigma_4)$$

и по теореме 11.15 это выражение должно быть ограничено величиной $N(4,2) = (2^4-2^2)/4=3$. Таким образом, так как $N(1, \sigma_4) = \sigma_4$, то

σ_4 не может быть больше 3, и если $\sigma_4=3$, то σ_1 и σ_2 должны быть равны нулю из-за членов $N(4, \sigma_1)$ и $N(2, \sigma_2)$ соответственно.

Подобные рассуждения могут быть использованы для того, чтобы установить границы, в которых могут находиться длины слов. Однако полученная граница не всегда удобна для применений (очевидно, утомительно перечислять все существенные множества $\{\sigma_i\}$, для которых существование синхронизируемого кода не исключается этой границей). (Напомним, что эта граница должна удовлетворяться для всех длин последовательностей, а не только для $n=4$.) Тем не менее если множество $\{\sigma_i\}$ таково, что граница (11.12) удовлетворяется для всех n, то может быть построен синхронизируемый код, имеющий эти σ_i (см. предыдущий §).

11.5. Максимальные синхронизируемые словари

Здесь будет показано, что выполнение неравенств теоремы 11.15 является достаточным, а также и необходимым условием для существования синхронизируемых кодов, т. е. можно построить синхронизируемый код, имеющий σ_i слов длины i, если неравенство (11.12) удовлетворяется при всех n. Эта конструкция вместе с тем дает коды, обладающие свойством префикса, определенным в гл. 10. Более жесткое ограничение, принятое в настоящей главе, конечно, приводит, вообще говоря, к меньшим словарям, чем в тех случаях, когда требуется лишь декодируемость.

Конструкция словаря будет следующая. Начнем со словаря D_0 с r словами, в котором каждый из r символов алфавита одновременно является словом. Если $\sigma_1=r$, то D_0 уже представляет собой требуемый словарь. Если $\sigma_1<r$ (ясно, что σ_1 не может быть больше r), то пусть L обозначает максимальное значение i, для которого $\sigma_i\neq 0$. Обозначим через $(D_0—w_0)$ множество слов, остающихся после того, как односимвольное слово w_0 будет устранено из D_0, и через $p(D_0—w_0)$ — множество, образующееся с помощью приписывания в начале каждого слова из $(D_0—w_0)$ префикса, представляющего собой последовательность символов p. То есть если $D_0=\{a, b, c, d...\}$, тогда $p(D_0—a)=\{pb, pc, pd,...\}$.

Словарь D_1 определяется как объединение множеств $D_1=(D_0—w_0)+w_0(D_0—w_0)+w_0w_0(D_0—w_0)+ \ldots +w_0w_0 \ldots w_0(D_0—w_0)$, где префикс максимальной длины $w_0w_0...w_0$ состоит из $L—1$ символов w_0. Выбор слова w_0 произволен. Так, например, если $r=3$, $L=4$, то

$D_0=\{0, 1, 2\}$; $0(D_0=0)=\{01, 02\}$; $00(D_0—0)=\{001, 002\}$;
$000(D_0—1)=\{0001, 0002\}$.

В общем случае i-я итерация этого процесса состоит в отыскании наименьшего значения j, такого, что число слов в D_{i-1} длины j

больше, чем σ_j, выбора произвольного слова w_{i-1} длины j из D_{i-1} и использовании его в качестве префикса для построения D_i по правилу

$$D_i = (D_{i-1} - w_{i-1}) + w_{i-1}(D_{i-1} - w_{i-1}) + w_{i-1}w_{i-1}(D_{i-1} - w_{i-1}) + \ldots$$
$$\ldots + w_{i-1}w_{i-1}\ldots w_{i-1}(D_{i-1} - w_{i-1}).$$

Самый длинный префикс $w_{i-1}w_{i-1}\ldots w_{i-1}$ должен быть таким, чтобы самое короткое слово из множества $w_{i-1}w_{i-1}\ldots w_{i-1}(D_{i-1} - w_{i-1})$ имело длину, не меньшую, чем $L-j+1$, так как использование более длинного префикса привело бы только к словам, имеющим бо́льшую максимальную длину. Этот процесс, который будем называть *префиксной процедурой построения,* оканчивается тогда, когда число слов каждой длины j при последней итерации будет равным или большим σ_j.

9 Продолжая предыдущий пример, предположим, что $r=3$, $L=4$, $\sigma_1=1$, $\sigma_2=2$, $\sigma_3=6$, $\sigma_4=9$ и $\sigma_j=0$ для $j>4$. Неравенства (11.12), как легко проверить, действительно удовлетворяются этим множеством $\{\sigma_i\}$. Словарь D_1 определяется, как и выше. Так как он содержит два слова длины единица и так как $\sigma_1=1$, то выберем слово $w_1=1$ в качестве префикса и построим D_2 следующим образом:

$$D_2 = \{2, 01, 02, 001, 002, 0001, 0002, 12, 101, 102, 1001, 1002, 112,$$
$$1101, 1102, 1112\}.$$

Так как D_2 содержит три слова длины 2 и так как $\sigma_2=2$, то выберем слово $w_2=01$ в качестве префикса и построим D_3 следующим образом:

$$D_3 = \{2, 02, 001, 002, 0001, 0002, 12, 101, 102, 1001, 1002, 112, 1101,$$
$$1102, 1112, 012, 0102, 0112\}.$$

Словарь D_3 содержит одно слово длины единица, два слова длины два, шесть слов длины три и девять слов длины четыре. Описанные ранее условия удовлетворяются, и построение оканчивается. Как было упомянуто ранее, это построение дает коды, обладающие свойством префикса. Это утверждение легко доказать по индукции.

Теорема 11.16. Все кодовые словари, определяемые префиксной процедурой построения, описанной выше, обладают свойством префикса.

Доказательство. Очевидно, что словарь D_0 обладает свойством префикса, так как все его слова имеют длину один. Предположим, что D_i обладает свойством префикса, и пусть w_i используется в качестве префикса при построении D_{i+1}. Тогда все слова из D_{i+1} имеют вид $w_iw_i\ldots w_iw_\nu$, где w_ν — слово из D_i, а число повторений префикса w_i произвольно. Если слово $w_iw_i\ldots w_iw_\nu$ из D_{i+1} является префиксом некоторого другого слова $w_iw_i\ldots w_iw_\mu$, то либо $w_iw_i\ldots w_iw_\nu$ должно быть префиксом w_μ, либо w_ν должно быть префиксом $w_iw_i\ldots w_iw_\mu$ (например, если $w_iw_iw_\nu$ — префикс w_iw_μ, то

$w_i w_\nu$ — префикс w_μ). В любом из этих двух случаев одно из слов w_i, w_μ или w_ν должно было быть префиксом одного из других, что противоречит гипотезе о том, что D_i обладает свойством префикса. Таким образом, по индукции все такие словари должны обладать свойством префикса, что требовалось показать. ■

Теперь мы должны показать, что, во-первых, эта процедура построения фактически приводит к синхронизируемым кодам и, во-вторых, с помощью этого метода можно получить по меньшей мере σ_i кодовых слов длины i при условии, что все неравенства (11.12) удовлетворяются для множества длин $\{\sigma_i\}$.

Для того чтобы доказать первое из этих двух утверждений, опишем сначала алгоритм установления синхронизации для этого класса кодов. Пусть D_i определяется, как и ранее, и пусть D_ν — фактически используемый словарь. Пусть далее D'_i *(расширение* D_i*)* определяется как словарь, который получается на i-м шаге префиксной процедуры построения, если не накладывается никаких ограничений на длину максимального слова. Для примера, рассмотренного выше, $D'_0=D_0$, но $D'_1=D_1+\{00001, 00002, 000001, 000002...\}$ и т. д., и каждый из словарей D'_i, $i>0$ содержит бесконечное число слов.

Рассмотрим теперь произвольную последовательность слов из D_ν возможно начинающуюся суффиксом из D_ν . Эта последовательность, очевидно, может быть разбита на слова из D'_0 с помощью запятых, помещаемых после каждого принятого символа. Затем для того, чтобы разбить последовательность на слова из D'_1, необходимо лишь отбросить запятые, поставленные после каждого появления слова w_0, которое используется при построении D_1 с помощью D_0. Ибо, если любое слово, кроме w_0, принадлежит D'_1, то и любое слово вида $w_0 w_0 \ldots w_0 w_\mu$ с $\mu \neq 0$ также принадлежит D'_1. Продолжая эту процедуру и на i-м шаге отбрасывая те запятые, которые поставлены после каждого слова w_{i-1}, можно последовательно разделить принимаемую последовательность на слова из $D'_0, D'_1, \ldots, D'_{\nu-1}$ и, наконец, на слова из D'_ν.

Если принимаемая последовательность, на самом деле, начинается полным словом из D_ν , очевидно, что эта процедура правильно разобьет эту последовательность на слова из D_ν . Если бы было не так, то было бы возможно декодировать последовательность как две различные последовательности слов из D'_ν , что запрещено свойством префикса D'_ν . (Заметим, что теорема 11.16 не накладывает никаких ограничений на длины слов, остающихся в каком-либо из словарей D_i.) Если, однако, принимаемая последовательность начинается суффиксом из D_ν , то запятая, поставленная после этого суффикса, могла бы быть устранена. Это, в свою очередь, меняет форму принимаемого первого слова и, как следствие, приводит к устранению запятой, следующей за первым фактически принятым словом. Это ошибочное устранение запятых может продолжаться дальше; если устраняется запятая, следующая за j-м принятым словом на некотором шаге, то запятая, следующая за

$(j+1)$-м принятым словом, может быть устранена на некотором последующем шаге. Свойство префикса D'_ν гарантирует, что никакое слово не является префиксом другого слова. Однако оно не гарантирует того, что одно слово не может содержаться в другом слове или что суффикс одного слова не может быть префиксом другого. Тем не менее свойство префикса гарантирует, что запятая, следующая за каким-либо словом из $D_{\nu 0}$, не будет устранена, кроме как *после* устранения запятой, предшествующей ей. Устранение идущей сзади запятой до ведущей запятой (или одновременно с ней) было бы возможным лишь, если слово из D'_ν также было бы префиксом из D'_ν. Таким образом, так как требуется лишь ν шагов для того, чтобы разделить принимаемую последовательность на слова из D'_ν, то запятая, следующая за ν-м принятым словом, не будет устранена. Начиная с этого места, последовательность будет правильно разделяться на слова из D_ν опять вследствие того, что этот словарь обладает свойством префикса. Следовательно, максимальная синхронизационная задержка ограничена величиной $\nu L+L-1$, где L обозначает длину максимального слова из D_ν, а $L-1$, очевидно, представляет собой длину наибольшего возможного суффикса из D_ν.

Таким образом, доказана следующая теорема.

Теорема 11.17. Словари D_ν, определяемые префиксной процедурой построения, являются синхронизируемыми с синхронизационной задержкой, не большей, чем $(\nu+1)L-1$ символов.

Остается доказать второе из сформулированных выше утверждений относительно этих словарей, т. е. о том, что в действительности они являются максимальными.

Теорема 11.18. Можно построить словари вида D_i, имеющие σ_j слов длины j, для любого множества целых чисел $\{\sigma_i\}$, удовлетворяющих границам (11.12).

Доказательство этой теоремы проводится очень легко с помощью следующей леммы.

Лемма 11.6. Если словарь D_i строится из словаря D_{i-1} при использовании слова w_{i-1} длины k в качестве префикса, то граница (11.12) удовлетворяется со знаком равенства для всех $n=k+1$, $k+2,\ldots, L$ (L вновь обозначает длину самого длинного кодового слова, остающегося в каком-либо из словарей D_i).

Доказательство. Единственными последовательностями слов, которые могут быть построены из слов словаря D_{i-1}, а не из слов D_i, являются те, которые оканчиваются словом w_{i-1}. Все такие последовательности, имеющие длину, большую, чем k, имеют вид

$$w_\alpha w_\beta \ldots w_{i-1}, \tag{11.13}$$

где w_l — слова из D_{i-1}. Если $w_l \neq w_{i-1}$ для некоторого w_l из этой последовательности и общая длина последовательности не больше, чем L, то некоторая циклическая перестановка (11.13) является последовательностью слов, оканчивающейся w_l, и является такой, которая может быть построена из слов D_i. Если последовательность (11.13) состоит только из слов w_{i-1}, то она принадлежит вырожденному классу эквивалентности. Отсюда следует, что все невырожденные классы эквивалентности, представляемые последовательностями слов из D_{i-1} с общей длиной n, где $k+1 \leqslant n \leqslant L$, также представляются последовательностями слов из D_i. Все границы (11.12), которые удовлетворяются на словаре D_{i-1} для $k+1 \leqslant n \leqslant L$, также удовлетворяются на D_i. Наконец, так как границы (11.12) удовлетворяются, очевидно, со знаком равенства для всех n на словаре D_0 и так как процедура построения такова, что длина префиксов, используемых при переходе от D_{i-1} к D_i, является неубывающей функцией i, то доказательство леммы следует по индукции. ■

Докажем теперь теорему 11.18.

Доказательство. Пусть $s^i{}_j$ — число слов длины j из D_i. Если $\sigma_1 = r$, то D_0 является требуемым словарем и теорема доказана. Если $\sigma_1 < r$, то D_1 строится с помощью слова (символа) из D_0 в качестве префикса, как было описано. Это построение можно продолжить до тех пор, пока не будет выполняться равенство $\sigma_1 = s^i{}_1$. В общем случае слова длины j используются в качестве префиксов для того, чтобы построить словарь D_i до тех пор, пока $s^i{}_j = \sigma_j$. Для того чтобы процесс продолжался до тех пор, пока все необходимые слова не будут построены, нужно показать, что если $s^i{}_j = \sigma_j$ для всех $j = 1, 2, \ldots, k$, то $s^i{}_{k+1} \geqslant \sigma_{k+1}$. Если бы это было неверно, то никакой из словарей D_l, $l > i$ не содержал бы достаточного количества слов длины $k+1$. Если это условие выполняется, то по индукции будет существовать некоторый словарь D_l, такой, что $s^l{}_j \geqslant \sigma_j$ для всех j, и теорема доказана. Но из леммы 11.6 известно, что словарь D_i (построенный из D_{i-1} при использовании префикса длины k) является таким, что

$$\sum_S N[s(P), s^i_\mu\, s^i_\nu \ldots s^i_\eta] = N(k+1, r). \tag{11.14}$$

Согласно гипотезе имеем

$$\sum_S N[s(P), \sigma_\mu\, \sigma_\nu \ldots \sigma_\mu] \leqslant N(k+1, r). \tag{11.15}$$

Лишь слова длины $k+1$ или меньшей могут быть включены в последовательность с общей длиной (числом символов) $k+1$. Так как $\sigma_j = s^i{}_j$ для всех j из интервала $1 \leqslant j \leqslant k$, то единственными членами в обеих суммах (11.14) и (11.15), которые не равны, будут те, которые включают в себя σ_{k+1} и $s^i{}_{k+1}$. Так как $N(1, \sigma_{k+1})$ и $N(1, s^i{}_{k+1})$ являются единственными такими членами, то, устраняя одинаковые члены из обеих частей неравенства

$$\sum_S N[s(P), \sigma_\mu\, \sigma_\nu \ldots \sigma_\eta] \leqslant N(k+1, r) = \sum_S N[s(P), s^i_\mu\, s^i_\nu \ldots s^i_\eta],$$

получаем $N(1, \sigma_{k+1}) \leqslant N(1, s^i{}_{k+1})$ и, следовательно, $\sigma_{k+1} \leqslant s^i{}_{k+1}$, что и требовалось доказать. ■

Теорема 11.19. Число слов σ_i длины i, $1 \leqslant i \leqslant L$, порождаемых префиксной процедурой построения, равно коэффициенту при x^i многочлена

$$P(x) = 1 - \frac{1 - rx}{(1-x)^{\alpha_1}(1-x^2)^{\alpha_2}(1-x^3)^{\alpha_3}\dots(1-x^l)^{\alpha_l}\dots} = \sum_{j=1}^{\infty}\sigma_j x^j, \qquad (11.16)$$

где α_i обозначает число слов длины i, использованных в качестве префиксов при построении последнего словаря.

Доказательство. Прежде всего, заметим, что выражение (11.16) справедливо для всех значений L длины слов максимальной длины, сохраняющихся в процедуре построения. Следовательно, величины σ_j, $j>L$ представляют собой число слов длины j, которые были бы в словаре, сохраняющем эти слова (т. е. числа слов длины j в расширении рассматриваемого словаря). Имея это в виду, определим $P(x)=\sum\limits_{j=1}^{\infty}\sigma_j x^j$ и покажем, что $P(x)$ задается равенством (11.16).

Пусть $P_\nu(x)$ имеет вид $\sum\limits_{j=1}^{\infty}\sigma_j(\nu)x^j$, где $\sigma_j(\nu)$ — число слов длины j в словаре D_ν (словаре, полученном, когда некоторое слово из $D_{\nu-1}$ используется в качестве префикса для построения нового словаря, как описывалось выше). Тогда число слов длины j в $D_{\nu-1}-w_{\nu-1}$) представляется коэффициентом при x^j в многочлене $P_{\nu-1}(x)-x^l$, где l — длина $w_{\nu-1}$. Аналогично число слов различных длин в множестве $w_{\nu-1}w_{\nu-1}\dots w_{\nu-1}(D_{\nu-1}-w_{\nu-1})$ задается многочленом $x^{\mu l}[P_{\nu-1}(x)-x^l]$, где μ — число повторений префикса $w_{\nu-1}$. Таким образом,

$$P_\nu(x) = [P_{\nu-1}(x) - x^l]\sum_{\mu=0}^{\infty} x^{\mu l} = \frac{P_{\nu-1}(x) - x^l}{1-x^l} = 1 - \frac{1 - P_{\nu-1}(x)}{1-x^l},$$

так что $1-P_\nu(x) = (1-P_{\nu-1}(x))/(1-x^l)$ и по индукции

$$1 - P(x) = \frac{1 - P_0(x)}{(1-x)^{\alpha_1}(1-x^2)^{\alpha_2}\dots(1-x^l)^{\alpha_l}}.$$

Так как $P_0(x)=rx$, то теорема доказана. ■

Рассмотрим пример, когда $r=3$, $\alpha_1=2$ и $\alpha_2=1$ (этот случай был рассмотрен ранее), имеем

$$P(x) = 1 - \frac{1-3x}{(1-x)^2(1-x^2)} = x + 2x^2 + 6x^3 + 9x^4 + 15x^5 + \dots$$

Интересно заметить, что в этом рассуждении не используются никакие предположения относительно порядка использования префиксов, они не обязательно используются в порядке возрастающей длины. Теорема 11.17 также не учитывает какого-либо частного упорядочения префиксов. В качестве следствия получаем, что рассмотренный алгоритм приводит к максимальным синхронизируемым словарям независимо от порядка устранения префикса. Повторим построение словаря с $r=3$, $\sigma_1=1$, $\sigma_2=2$, $\sigma_3=6$ и $\sigma_4=9$, устраняя префиксы в порядке, отличном от использованного ранее. Получим:

$$D_0=\{0,\ 1,\ 2\};$$

$$D_1=\{1,\ 2,\ 01,\ 02,\ 001,\ 002,\ 0001,\ 0002\};$$

$$D_2=\{1,\ 2,\ 02,\ 001,\ 002,\ 0001,\ 0002,\ 011,\ 012,\ 0102\};$$

$$D_3=\{2,\ 02,\ 001,\ 002,\ 0001,\ 0002,\ 011,\ 012,\ 0102,\ 12,\ 102;\ 1001,\ 1002,\ 1011,\ 1012,\ 112,\ 1102,\ 1112\}.$$

Хотя этот словарь является синхронизируемым и содержит то же число слов каждой длины, что и соответствующий словарь рассмотренного ранее примера, эти два словаря не тождественны.

Если цель состоит в построении синхронизируемого словаря, имеющего максимально возможное число слов длины, не превосходящей L, то она, очевидно, может быть достигнута при использовании самого короткого слова в качестве префикса на каждом шаге построения. [Это означает, что каждое слово длины l из интервала $L-(\nu+1)j<l\leqslant L-\nu j$ в множестве $(D_{i-1}-w_{i-1})$ дает ν слов длины, не превосходящей L, принадлежащих D_i, когда w_{i-1} имеет длину j. Очевидно, что добавляемое число слов является невозрастающей функцией j.] Общее число слов длины L (или меньшей) в D_i будет не меньше, чем число таких слов в D_{i-1}, тогда и только тогда, во-первых, когда длина j использованного префикса не больше, чем $[L/2]$, и, во-вторых, когда при четном L имеются, по меньшей мере, два слова в D_{i-1} с длиной $L/2$. Если L нечетное, то все слова длины $(L-1)/2$ могут быть использованы в качестве префиксов всех слов длины $(L+1)/2$ так, что число слов в D_i никогда не будет меньше числа слов в D_{i-1}, если $j\leqslant(L-1)/2$. Если L четное, то до тех пор, пока имеются, по крайней мере, два слова длины $L/2$, одно из них может быть устранено и использовано в качестве префикса другого без уменьшения общего числа слов длины L и меньше. В соответствии с этим, когда L нечетное, никакие слова длины, меньшей, чем $(L+1)/2$, не остаются в последнем словаре D_i, в то время как при четном L он будет включать в себя лишь одно слово длины $L/2$ и ни одного с меньшей длиной. Все последовательности слов с полной длиной n из интервала $[L/2]+1\leqslant n\leqslant L$ должны состоять из одного слова. Но согласно лемме 11.6 число таких последовательностей равно числу невырожденных классов эквивалентности по символам для всех n из этого интервала. Таким образом, общее число слов в окончательном словаре точно равно $\sum\limits_{n=[L/2]+1}^{L} N(n,\ r)$ плюс одно оставшееся слово длины $L/2$, когда L четное. Этот результат сформулирован в следующей теореме.

Теорема 11.20. Максимальное число слов длины L или меньшей в синхронизируемом словаре

$$N_L = \frac{1+(-1)^L}{2} + \sum_{n=[L/2]+1}^{L} N(n, r).$$

Если бы использовались лишь слова длины L, то число слов просто было бы равно $N(L, r)$.

Очевидно, что конструкция максимальных синхронизируемых словарей, рассмотренное в этом параграфе, не является единственно возможным. Суффиксная конструкция, например, в которой выброшенные слова используются в качестве суффиксов, а не в качестве префиксов, была бы столь же эффективна. Конструкция, рассмотренная здесь, обладает свойством префикса со свойственными ему преимуществами, которые были указаны в гл. 10.

В заключение докажем еще одно интересное свойство расширенных словарей D'_0, определенных ранее.

Теорема 11.21. Расширенные словари D'_ν, полученные с помощью префиксной процедуры построения, являются полными.

Доказательство. Теорему легко доказать по индукции. Очевидно, что D'_0 является полным. Так как D'_ν обладает свойством префикса, то этот словарь полный тогда и только тогда, когда $\sum\limits_{i=1}^{\infty} r^{-l_i(\nu)} = 1$, где $l_i(\nu)$ — длина i-го слова из D'_ν (ср. с теоремой 10.4). Предположим, что D'_μ является полным. Тогда, так как каждое слово длины $l_i(\mu)$ в D'_μ (исключая w_μ) дает одно слово длины $l_i(\mu)+jl_\mu(\mu)$ в $D'_{\mu+1}$ при всех $j=0, 1,\ldots$ (где $l_\mu(\mu)$ — длина w_μ), то

$$\sum_{i=1}^{\infty} r^{-l_i(\mu+1)} = \sum_{j=0}^{\infty}\sum_{i\neq\mu} r^{-[l_i(\mu)+j\,l_\mu(\mu)]} = \frac{\sum\limits_{i\neq\mu} r^{-l_i(\mu)}}{1-r^{-l_\mu(\mu)}} = 1,$$

и теорема доказана.

Таким образом, если не накладывается никаких ограничений на длину максимального слова, то синхронизируемые словари могут удовлетворять со знаком равенства границе, выведенной ранее для менее ограниченных декодируемых словарей. Однако следует отметить, что в то время, как могут быть построены декодируемые словари, имеющие любое множество длин слов, удовлетворяющих этой границе, длины слов в синхронизируемом словаре удовлетворяют ограничению, выраженному неравенствами (11.12). Более того, синхронизационная задержка, соответствующая расширенным словарям D'_ν, не ограничена для всех $\nu>0$, так как сама длина слова является неограниченной (ср. с теоремами 11.6 и 11.17).

Глава 12

СИНХРОНИЗИРУЕМЫЕ БЛОКОВЫЕ КОДЫ

12.1. Введение

Если наложено ограничение, чтобы все кодовые слова в словаре имели одну и ту же длину, то такой код обычно называется *блоковым кодом* (ср. с § 10.1). Очевидно, что блоковый код является декодируемым. Более того, результаты § 11.5 также показывают, как построить максимальные синхронизируемые словари в этом частном случае. Тем не менее часто требуется наложить дополнительные ограничения на синхронизируемые словари. Может быть полезным наложение более жесткого ограничения, например, на допустимую синхронизационную задержку, или дальнейшее сужение класса словарей для того, чтобы упростить синхронизацию и процедуру декодирования, связанные с кодом. В этой главе исследуются некоторые методы, позволяющие достичь эти различные цели. Начнем с построения синхронизируемых блоковых кодовых словарей, для которых синхронизационная задержка значительно меньше той, которая гарантируется общей конструкцией из § 11.5.

12.2. Коды без запятой

Пусть D будет блоковым кодовым словарем, содержащим слова w_i, $i=1, 2, \ldots, N$, где

$$w_i = \omega_1^i \omega_2^i \ldots \omega_n^i . \tag{12.1}$$

Стыком слов w_i и w_j назовем любую n-последовательность вида

$$\omega_{k+1}^i \omega_{k+2}^i \ldots \omega_n^i \omega_1^j \omega_2^j \ldots \omega_k^j \tag{12.2}$$

для любого k из интервала $1 \leqslant k \leqslant n-1$. Словарь D называется словарем *без запятой* тогда и только тогда, когда никакой стык любых двух (не обязательно различных) слов из D сам не является словом из D. Пусть $p^i{}_k = \omega^i{}_1 \omega^i{}_2 \ldots \omega^i{}_k$ обозначает префикс, а $s^i{}_{n-k} = \omega^i{}_{k+1} \omega^i{}_{k+2} \ldots \omega^i{}_n$ обозначает суффикс слова w_i при некотором k из интервала $1 \leqslant k \leqslant n-1$. Тогда следующее определение, очевидно, эквивалентно определению словаря без запятой. Словарь D будет словарем без запятой тогда и только тогда, когда для каждого префикса $p^i{}_k$ и каждого суффикса $s^i{}_{n-k}$, таких, что $w_i = p^i{}_k s^i{}_{n-k}$ является словом из словаря D, либо $p^i{}_k$ не является суффиксом из D, либо $s^i{}_{n-k}$ не является префиксом из D.

Очевидно, что словарь без запятой D является синхронизируемым с синхронизационной задержкой самое большее $2n-1$ символов (где n длина слова). Для любой последовательности слов из D никакой стык слов не может быть перепутан с кодовым словом. Как только наблюдается кодовое слово, устанавливается синхронизация. Но любая последовательность длины $2n-1$ должна содержать одно полное слово, так что максимальная задержка равна $2n-1$. В действительности эта задержка может быть уменьшена на один символ, учитывая, что если $2n-2$ последовательных символов не содержат слова, то слово обязательно должно начинаться n-м принятым символом.

Максимальное число n-символьных слов из r-ичного алфавита в синхронизируемом словаре, как было найдено в § 11.4, ограничено величиной

$$N(n, r) = \frac{1}{n} \sum_{d \mid n} \mu(d)\, r^{n/d}\,. \tag{12.3}$$

Эта граница применима также к кодам без запятой. Так как «свобода от запятой» является значительно более жестким ограничением по сравнению с только синхронизируемостью, можно было бы предположить, что эта граница не может, вообще говоря, достигаться в классе кодов без запятой. Но, как сейчас будет показано, в действительности могут быть построены коды без запятой с $N(n, r)$ словами для всех нечетных значений n. Хотя были найдены также некоторые коды без запятой с $N(n, r)$ словами четной длины, не существует общей конструкции для таких кодов. В действительности никакая общая конструкция для всех четных n невозможна, так как известны множества параметров n и r, для которых эта граница не может быть достигнута. Максимальное число слов, например, в словаре без запятой со словами из двух символов в алфавите из четырех символов известно и равно пяти, в то время как $N(2, 4)=6$. Максимальный словарь с $n=4$, $r=4$ содержит 57, а не $N(4, 4)=60$ слов; другие контрпримеры, включая бесконечный ряд значений n и r, для которых граница (12.3) не может быть достигнута, также были найдены.

Построение максимальных кодов без запятой нечетной длины, которое здесь будет описано, является просто переложением префиксной процедуры построения из § 10.5. Дополнительное условие состоит в том, что на каждом шаге построения префиксное слово w_i должно быть самым коротким словом *нечетной длины*, остающимся в D_i. (Если имеется несколько слов этой длины, то может быть выбрано любое из них.) Как уже было показано (лемма 11.6), граница (11.12) удовлетворяется со знаком равенства для слов из D_i при всех $n=l+1, l+2, \ldots, L$, где l — длина префиксного слова w_{i-1}. Таким образом, продолжая префиксную процедуру построения до тех пор, пока самое короткое слово, остающееся в D_ν, будет длины l для любого l из интервала $(n+1)/2 \leqslant l \leqslant n \leqslant L$, получим, что

$$\sum_{s} N\,[s(P),\ \sigma_i\,\sigma_j \ldots \sigma_k] = N(1,\ \sigma_n) = \sigma_n = N(n,\ r) \tag{12.4}$$

[ср. с (11.12)] и число σ_n слов длины n из D в действительности равно $N(n,\ r)$. Требуемый словарь $D(n,\ r)$ получается выбрасыванием из D_ν всех слов, кроме тех, которые имеют длину n. То, что $D(n, r)$ является синхронизируемым с конечной задержкой, сразу следует из § 11.5. Однако, как показано в следующей теореме, он на самом деле является словарем без запятой.

Теорема 12.1. Словарь $D=D(n, r)$ с n-символьными словами из r-ичного алфавита, определенный выше, является словарем без запятой для любого нечетного целого n и любого целого r.

Доказательство. Так как слова в D имеют нечетную длину, то стыковое слово может совпадать с кодовым словом, только если некоторый префикс четной длины из D является также суффиксом в D. Следовательно, для того чтобы показать, что D — словарь без запятой, нужно лишь показать, что это событие не может иметь места.

Пусть p — префикс четной длины из D и w — n-последовательность, имеющая p в качестве суффикса. Так же, как и в § 11.5, поставим запятую после каждого символа как в p, так и в w, и затем последовательно будем устранять их. На j-м шаге устраняются те запятые, которые поставлены после каждого слова w_j, использованного при построении D_{j+1} по D_j. После каждого такого шага w и p могут быть выражены в следующем типичном виде:

$$w = \;.\,.\,.\underset{c_{l+1}}{,}\;.\,.\,.\,.\,.\,.\,.\,.\underset{c_l}{,}\;.\,.\,.\,.\underset{c_{l-1}}{,}\;.\,.\,.\underset{c_{l-2}}{,}\;.\,.\,.\underset{c_0}{,}\;.\,.\,.\,,$$

$$p = \underset{c^*_l}{,}\;.\,.\,.\,.\,.\,.\,.\,.\underset{c^*_{l-1}}{,}\;.\,.\,.\underset{c^*_{l-2}}{,}\;.\,.\,.\,,\;.\,.\,.\,.\,,\;.\,.\,.\underset{c^*_0}{,} \tag{12.5}$$

где c_i и $c^*{}_i$ обозначают числа символов между i-й запятой (справа) и самой крайней справа запятой в w и p соответственно, а точки обозначают сами символы. [Удобно различать запятые в w и p по их расположениям: из контекста будет ясно, используется ли c_i (или $c^*{}_i$) как отметка для i-й запятой в w (или в p) или как число, соответствующее ее положению]. После того как будет устранена какая-либо запятая, остающиеся запятые переобозначаются вновь для согласования с этими правилами, а l переопределяется так, чтобы $c^*{}_l$ всегда соответствовало запятой, предшествующей префиксу, как показано в (12.5).

Доказательство состоит в демонстрации того, что если запятые одновременно устраняются из w и p в соответствии с упомянутой выше процедурой, то c_0 будет устранено одновременно с $c^*{}_0$. Так как p является префиксом, то $c^*{}_0$ в конце концов, должно быть устранено; поэтому, так как c_0 также устраняется, w не может быть кодовым словом. Для начала заметим, что если $c_\nu = c^*_\nu$ на любом этапе процедуры устранения запятых, то $c_i = c^*_i$ для всех $i < \nu$. Далее, так как p является префиксом и так как при построении $D(n, r)$ были использованы в качестве префиксов лишь слова нечетной длины, то $c^*_l - c^*_{l-1}$ должно быть нечетным. Будь это не так, c^*_{l-1} нельзя было бы никогда устранить, и p имело бы слово из D_ν в качестве префикса, что невозможно, в силу того, что D_ν обладает свойством префикса (см. § 11.5).

Покажем далее, что после каждого шага в процедуре устранения запятых остающиеся запятые будут иметь одну из трех конфигураций:

1. $c_l = c^*_l$;

2. $c_l > c^*_l$, $c_{l-1} = c^*_{l-1}$;

3. $c_l < c^*_l < c_{l+\nu}$, $c_{l-1} = c^*_{l-1}$ и $c_{l+i} - c_{l+i-1}$ четно для всех $i = 0$, 1, ..., $\nu - 1$.

В каждом случае c^*_l обозначает положение запятой, предшествующей p, как показано в (12.5).

Вначале, очевидно, запятые соответствуют конфигурации *1*. Если запятые соответствуют конфигурации *1* на j-м шаге и все запятые, кроме c_l, устранены, то они остаются соответствующими этой конфигурации. (Заметим, что c_ν и c^*_ν устраняются одновременно при любых $\nu < l$.) Если устраняется c_l, то они должны соответствовать тогда конфигурации *2*. Аналогично, если они соответствуют конфигурации *2*, то эта конфигурация будет сохраняться до тех пор, пока на некотором шаге не будет устранена c^*_{l-1} или c_{l-1}. Но c_{l-1} нельзя устранить ни на каком шаге. Это следует из того, что слова, использованные в качестве префиксов при построении D_{j+1} по D_j, были выбраны в порядке увеличивающейся (нечетной) длины. Так как $c_l - c_{l-1} > c^*_l - c^*_{l-1}$ и так как $c^*_l - c^*_{l-1}$ нечетны, то c^*_{l-1} была бы поэтому устранена до c_{l-1} и запятые тогда соответствовали бы конфигурации *3*. Более того, c^*_{l-1} не будет устранена ни при какой конфигурации (в предположении, что c^*_0 уже не была устранена), если только $c^*_{l-1} - c^*_{l-2}$ (и, следовательно, $c_{l-1} - c_{l-2}$) не является четным. Если $c^*_{l-1} - c^*_{l-2}$ нечетно, то $c^*_l - c^*_{l-2}$ будет четным, и c^*_{l-2} не может быть, следовательно, устранена, и p не может быть префиксом из D. В результате, если c^*_{l-1} устранена и конфигурация *2* перешла к конфигурации *3*, то (если запятые переобозначены) $c_l - c_{l-1}$ будет четным. Дальнейшие устранения запятых, обозначенных c^*_{l-1}, приводят к общему условию, соответствующему конфигурации *3*. Таким образом, соответствуя конфигурации *3*, c_{l-1} не может быть устранена до c_l. Запятые, следовательно, будут оставаться в этой конфигурации до тех пор, пока не будет устранена c_l, и в этом случае они возвратятся к конфигурации *2*.

Существенным во всем этом является то, что после каждого шага процедуры устранения запятых c_{l-1} и c^*_{l-1} будут совпадать, по крайней мере, до того, как устраняется c^*_0. (Следует помнить, что после устранения каждой запятой l переопределяется так, чтобы c^*_l всегда соответствовала запятой, предшествующей p.) В соответствии с этим, так как w и p должны содержать, по меньшей мере, одну запятую в одинаковых местах слева от c_0 и c^*_0, то c_0 будет устраняться одновременно с c^*_0. Исключением из этого утверждения был бы случай, когда c^*_{l-1} и c^*_0 совпадают. Но так как $c^*_l - c^*_{l-1}$ всегда нечетно, а $c^*_l - c^*_0$ всегда четно, то это невозможно, и утверждение остается справедливым. В конце концов, процедура устранения запятых приведет к устранению c_0 из w. Следовательно, w не может быть словом в D, никакой префикс четной длины из D не может также быть суффиксом в D, и D — словарь без запятой, что и требовалось доказать. ■

Таким образом, существуют максимальные словари без запятой для каждого нечетного целого n. К сожалению, доказательство этого факта хотя и является конструктивным, но не вселяет большой надежды на легкость реализации процедур кодирования и декодирования этих кодов. По этой причине полезно ввести дальнейшие ограничения на словарь с целью упрощения его реализации, принимая во внимание тот факт, что эти дополнительные ограничения несомненно приведут к уменьшению числа слов в словаре. Ряд таких ограничений будет исследован в нескольких последующих параграфах.

Ограничение, которое будет рассмотрено в следующем параграфе, накладывается не столько для того, чтобы упростить кодирование и декодирование получающихся кодов, сколько для того, чтобы уменьшить еще более число символов, необходимых для установления синхронизации. Словари, получаемые с этим ограничением, будут не только несколько более легкими для синхронизации по сравнению с обычными словарями без запятой, но также во многих случаях будут обладать неожиданными преимуществами, состоящими в более легком кодировании и декодировании, несмотря на то, что первоначальная цель наложения ограничений состояла в другом.

Однако до этого рассмотрим вновь ограничение, которому удовлетворяют коды без запятой для случая, когда длина слова n является четной. К сожалению, теорема 12.1 справедлива лишь для нечетных n. Как уже упоминалось ранее, доказано, что граница (12.1) не достигается для некоторых значений n и r, так что, очевидно, невозможно дать общую конструкцию для построения кодов без запятой четной длины, удовлетворяющих этой границе. Тем не менее существует относительно простая конструкция для словарей без запятой с четной длиной слов, которая приводит к кодам, параметры которых лежат вблизи этой границы.

Сначала построим словарь без запятой $D(2, r)$ с двухсимвольными словами. Разобьем r-символьный алфавит на три непересекающихся множества S_1, S_2 и S_3. Первый символ слова $w = \omega_1\omega_2$ из $D(2, r)$ должен быть либо из S_1, либо из S_2, но если ω_1 принадлежит S_1, то ω_2 должно быть либо из S_2, либо из S_3, а если ω_1 принадлежит S_2, то ω_2 должно быть из S_3. Легко установить для такого словаря, что он является словарем без запятой. Любой стык

должен иметь вид $\omega_2\omega_1$, где ω_2 принадлежит либо S_2, либо S_3, а ω_1 находится либо в S_1, либо в S_2. Никакой такой стык не может быть кодовым словом. Очевидно, что число кодовых слов в $D(2, r)$ максимизируется, если взять числа символов в каждом множестве по возможности равными. Таким образом, обозначая через $N(S_i)$ число символов в множестве S_i, получим:
$N(S_1)=[r/3]$, $N(S_2)=[(r+1)/3]$ и $N(S_3)=[(r+2)/3]$, где квадратные скобки обозначают целую часть заключенной в них дроби. При этом число слов в $D(2, r)$ будет равным

$$N(S_1)\{N(S_2)+N(S_3)\}+N(S_2)N(S_3)=\left[\frac{r^2}{3}\right]. \qquad (12.6)$$

Для того чтобы построить словарь без запятой с n-символьными словами, где $n=2m$, $m>1$, обозначим через S_4 подмножество слов из $D(2, r)$, а через S_5 — множество всех упорядоченных пар символов, не входящих в S_4 (т. е. S_4+S_5 содержит все r^2 различные пары символов ab). Словарь $D(2m, r)$ содержит все слова вида $a_1a_2...a_mb_1b_2...b_m$, где пара a_1b_1 принадлежит S_4, а пары a_ib_i, $i\neq 1$ принадлежат S_5. Словарь $D(2m, r)$, очевидно, также является словарем без запятой. Единственный стык, который мог бы быть словом из $D(2m, r)$, имеет вид $b_1b_2...b_ma_1a_2...a_m$, но то, что множество пар a_1b_1 само образует словарь без запятой, исключает эту возможность.

Используя те же обозначения, что и ранее, найдем, что число слов в $D(2m, r)$ будет равно $N(S_4)\{N(S_5)\}^{(n/2)-1}$. Если $n\geqslant 6$, можно считать, что $N(S_4)$ содержит $[r^2/(n/2)]$ элементов, что дает

$$\left[\frac{2r^2}{n}\right]\left\{r^2-\left[\frac{2r^2}{n}\right]\right\}^{(n/2)-1}$$

слов в $D(2m, r)$. Когда n велико, это выражение приближенно принимает вид

$$\frac{2r^n}{n}\left\{1-\frac{2}{n}\right\}^{n/2}>\frac{2r^n}{en}. \qquad (12.7)$$

Но из ф-лы (12.3)

$$N(n, r)<r^n/n \qquad (12.8)$$

для всех n, так что эта конструкция дает словари, содержащие, по меньшей мере, $100(2/e)\,\%\approx 73{,}5\,\%$ слов от теоретически возможного граничного значения.

12.3. Коды без запятой с инвариантными путями

Ограничение на кодовые слова в этом параграфе будет следующим. Если блоковый словарь D содержит n-символьные слова, то для однозначного установления синхронизации должно быть принято не более n последовательных символов. Ясно, что такие словари будут словарями без запятой. Однако они составляют более ограниченный класс, чем все коды без запятой, так как последние могут потребовать до $2n-1$ символов до установления синхронизации.

Для того чтобы описать конструкцию для словарей с этим свойством, введем понятия «путей» и «инвариантности путей». Для иллюстрации этих понятий рассмотрим код без запятой с параметрами $r=3$, $n=3$:

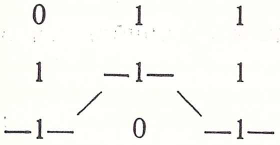
$$\{100, 101, 102, 200, 201, 202, 211, 212\}. \qquad (12.9)$$

Так как все слова в этом словаре имеют вид cba с $c>b$, $b\leqslant a$, то легко увидеть, что он является словарем без запятой, а так как $N(3, 3)=8$, то словарь является максимальным. Определим теперь *матрицу инцидентности* $r\times n$ из 0 и 1 : ij-м элементом матрицы будет 1, если i-й символ алфавита (при каком-либо упорядочении) появляется на j-й символьной позиции какого-либо слова, и 0, если это не так. Пусть первый символ алфавита словаря (12.9) будет 0, второй 1 и третий 2; поставим в соответствие этому словарю матрицу инцидентности:

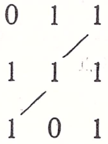
Символ	Позиция		
	1	2	3
0	0	1	1
1	1	1	1
2	1	0	1

(12.10)

Путем на матрице инцидентности называется линия, проходящая через одну 1 в каждом столбце, например,



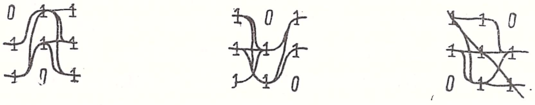
(12.11)



(12.12)

Имеется взаимооднозначное соответствие между n-последовательностями r-ичного алфавита и путями на матрице инцидентности, а именно: если путь проходит через элемент $a_{ij}=1$, то j-й символ n-последовательности является i-м символом алфавита. В матрице (12.11) путь соответствует слову 212; это слово из словаря без запятой (12.9). В матрице (12.12) путь соответствует слову 210, которое не принадлежит словарю.

Эта конструкция дает средства для проверки словаря на свойство «свободы от запятой». Рассмотрим стык, образующийся из суффикса (для слова) длины l и префикса (для слова) длины $n-l$. Все такие стыки соответствуют путям на матрице инцидентности, получающимся, когда последние l столбцов матрицы инцидентности словаря ставятся впереди ее первых $n-l$ столбцов (т. е. получаются с помощью циклической перестановки столбцов на l позиций вправо). Все первоначальные пути из j-го столбца к $(j+1)$-му столбцу остаются неизменными [j-й столбец в исходной матрице теперь будет $(j+l)$-м столбцом по модулю n], кроме, конечно, случая, когда $j+l=n$. Пути можно пополнить, соединив каждую единицу в l-м столбце переставленной матрицы с каждой единицей в $(l+1)$-м столбце. Это соответствует условию, что любой префикс может следовать за любым суффиксом. Эти «стыковые» матрицы проиллюстрированы ниже для словаря (12.9) вместе с самой матрицей инцидентности словаря; каждый путь соответствует слову или стыку слов:



$l=0$ $l=1$ $l=2$

(12.13)

Обозначим через M исходную матрицу инцидентности, а через P_M — множество путей на M, которые соответствуют кодовым словам. Обозначим далее через $M(j)$ матрицу M, циклически переставленную на j позиций вправо, и через $P_{M(j)}$ — множество путей на $M(j)$, таких, как были определены выше.

Теорема 12.2. Код является кодом без запятой тогда и только тогда, когда никакой из путей в множестве P_M не входит ни в какое множество $P_{M(j)}$.

Доказательство следует прямо из того, что имеется взаимооднозначное соответствие между каждым путем в P_M и кодовым словом и между каждым путем в $P_{M(j)}$ и стыком, состоящим из последних j символов одного слова, за которыми следуют первые $n-j$ символов другого слова. ■

Теорема 12.3. Словарь с n-символьными словами является синхронизируемым с задержкой, не большей, чем n символов, тогда и только тогда, когда никакой путь из какого-либо множества $P_{M(j_1)}$ не принадлежит никакому другому множеству $P_{M(j}$ j_1, $j_2=0, 1, 2, \dots, n-1$, $j_1 \neq j_2$.

Доказательство. Если множества $P_{M(j_1)}$ и $P_{M(j_2)}$, $j_1 \neq j_2$ содержат общие пути и если принимается соответствующая n-последовательность, то невозможно понять, является ли началом правильного слова (j_1+1)- или (j_2+1)-й символ. Наоборот, если никакой путь из одного множества не принадлежит какому-либо другому множеству, то любая n-последовательность, которая может быть составлена из последних j_1 символов одного слова, за которыми следуют первые $n-j_1$ символов второго слова, не может быть сформирована для какого-нибудь другого значения j. Таким образом, любая принятая n-последовательность однозначно устанавливает значение j и, следовательно, правильную синхронизацию. ■

В то время как теорема 12.2 предлагает метод определения того, является ли некоторый частный словарь словарем без запятой или нет, теорема 12.3 чрезвычайно полезна, если ее использовать в качестве основы алгоритма при построении более ограниченного класса кодов без запятой, как указывалось выше. Рассмотрим в связи с этим $(r \times n)$-матрицу M из единиц и нулей, обладающую тем свойством, что *все* пути, соединяющие единицы в последовательных столбцах, принадлежат множеству P_M и, следовательно, соответствуют кодовым словам. Словарь теперь полностью определяется его матрицей инцидентности M. Так как все возможные пути соответствуют кодовым словам, то множество P_M нет необходимости задавать явно. По этой причине такие коды называются *кодами с инвариантными путями*. Для нас представляют интерес коды с инвариантными путями, которые являются одновременно кодами без запятой. Такие коды, если они существуют, конечно удовлетворяют условию теоремы 12.2, и, кроме того, для них справедлива следующая теорема.

Теорема 12.4. Коды без запятой с инвариантными путями и длиной слов n имеют синхронизационную задержку самое большее n символов. Более того, любая циклическая перестановка кода без запятой с инвариантными путями представляет собой другой код без запятой с инвариантными путями.

Доказательство. Оба эти утверждения следуют из того, что все возможные пути во всех матрицах $M(j)$, $j=0, 1,..., n-1$ соответствуют кодовым словам или стыкам слов. Предположим, что путь в матрице $M(j_1)$ также является путем в матрице $M(j_2)$. Тогда путь в $M(j_1-j_2)$ будет также путем в матрице $M(0)=M$, и код не будет кодом без запятой. Таким образом, все пути во всех матрицах $M(j)$ являются одиночными, и согласно теореме 12.3 синхронизационная задержка самое большее равна n символам. То же самое рассуждение показывает, что каждая матрица $M(j)$ должна также соответствовать коду без запятой, и так как в матрице проведены все пути, то каждый такой код является кодом с инвариантными путями.

Следует подчеркнуть, что в общем случае словари без запятой не являются словарями с инвариантными путями. Путь в матрице (12.12), например, не соответствует никакому кодовому слову в словаре (12.9).

Одна из конструкций, которая порождает коды без запятой с инвариантными путями, состоит в следующем. Пусть c и d — два двоичных вектора-столбца и пусть $\bar{c}$ является дополнением к c. Рассмотрим теперь матрицу

$$M=\Big\{\overbrace{c\,\bar{c}\,\bar{c}\ldots\,\bar{c}}^{[n/2]\text{ столбцов}}\qquad\overbrace{d\,d\,\bar{c},\ldots d}^{[(n-1)/2]\text{ столбцов}}\Big\}\,. \tag{12.14}$$

Любая матрица $M(j)$, получаемая с помощью циклической перестановки столбцов M на j позиций вправо, такова, что либо ее первый столбец есть $\bar{c}$ (если $[(n-1)/2]+1 \leqslant j \leqslant n-1$), либо $(j+1)$-й столбец есть c (если $1 \leqslant j \leqslant [n/2]$). (Если n четно, то оба случая имеют место, когда $j=n/2$.) В каждом из этих двух случаев очевидно, что никакой путь в $M(j)$ не может также быть путем в M, так как, по крайней мере, один из столбцов M заменяется на его дополнение в $M(j)$. Следовательно, доказана следующая теорема.

Теорема 12.5. Матрица инцидентности (12.14) соответствует коду без запятой с инвариантными путями при любых выборах c и d.

Если c содержит l единиц, а d содержит m единиц, то имеются

$$l(r-l)^{[n/2]}\, m^{[(n-1)/2]} \tag{12.15}$$

различных путей в M и, следовательно, столько же различных слов в словаре. Для того чтобы максимизировать число кодовых слов, m следует, очевидно, положить равным r (d должно быть столбцом, состоящим лишь из единиц), а l следует выбрать так, чтобы

$$(l-1)(r-l+1)^{[n/2]} \leqslant l(r-l)^{[n/2]}; \tag{12.16}$$

$$(l+1)(r-l-1)^{[n/2]} < l(r-l)^{[n/2]}. \tag{12.17}$$

Если бы l была непрерывной переменной, то выражение $l(r-l)^{[n/2]}$ принимало бы максимальное значение, когда $l=r/(1+[n/2])$. Так как $l>0$, то для того, чтобы в словаре были какие-нибудь слова, оптимальное значение l должно быть равно единице всегда, когда $[n/2]+1\geqslant r$. Таким образом, всегда, если n настолько велико, что удовлетворяется это неравенство, то число кодовых слов равно

$$N_w=(r-1)^{[n/2]}\, r^{[(n-1)/2]}=\frac{n}{r}\left(1-\frac{1}{r}\right)^{[n/2]}\frac{r^n}{n}. \tag{12.18}$$

Отношение числа кодовых слов, которое дает эта конструкция, к числу кодовых слов в максимальном словаре без запятой стремится к нулю с ростом n. Основное преимущество словарей без запятой с инвариантными путями состоит в уменьшенной синхронизационной задержке и в получающейся отсюда возможности более простой реализации. Так, например, когда n достаточно велико для того, чтобы можно было приравнять l единице в ф-лах (12.16) и (12.17), синхронизация может быть достигнута путем поиска местонахождения символа, который во всех словах должен стоять на первом месте, и дальнейшей проверке того, появится ли такой же символ в какой-либо из следующих $[n/2]$ позиций. Если нет, то этот символ и будет соответствовать началу кодового слова.

Неожиданным преимуществом этих словарей перед обычными словарями без запятой является относительная простота их кодирования и декодирования. Чтобы продемонстрировать это, рассмотрим опять случай, когда l равно единице. Кодовые слова, определенные матрицей (12.14), все начинаются каким-то одним фиксированным символом, за которым следуют $[n/2]$ символов, каждый из которых может быть любым символом алфавита, но не этим начальным, и за ними следуют $[(n-1)/2]$ символов, на которые не наложены никакие ограничения. Следовательно, информация может быть отображена в последовательность чередующихся $[(n-1)/2]$-последовательностей, составленных из r-символьного алфавита и $[n/2]$-последовательностей, составленных из $(r-1)$-символьного алфавита. Операции кодирования и декодирования поэтому легко реализовать.

12.4. Префиксные коды

Дальнейшее ограничение на словари, которое будет исследовано, также вводится для упрощения синхронизации путем ограничения числа символов, необходимых для определения правильной синхронизации. Оно состоит в использовании одной и той же m-последовательности в качестве префикса перед каждым кодовым словом с n символами. Синхронизация устанавливается после обнаружения этого префикса в некотором месте принимаемой последовательности. Чтобы быть уверенным в том, что этот префикс всегда указывает начало слова, необходимо запретить появление этого префикса в качестве части кодового слова или стыка кодового слова и префикса. Это означает, что если префикс состоит из m символов $\gamma_1\gamma_2\gamma_3\ldots\gamma_m$, а кодовое слово имеет вид $\gamma_1\gamma_2\ldots\gamma_m\alpha_1\alpha_2\alpha_3\ldots\alpha_n$, то ни одна из m-последовательностей

$$\begin{aligned}
&\gamma_{i+1}\gamma_{i+2}\cdots\gamma_m\alpha_1\ldots\alpha_i, && 1\leqslant i\leqslant m-1;\\
&\alpha_{i+1}\alpha_{i+2}\cdots\alpha_{i+m}, && 0\leqslant i\leqslant n-m;\\
&\alpha_{i+1}\alpha_{i+2}\cdots\alpha_n\gamma_1\cdots\gamma_{i+m-n}, && n-m+1\leqslant i\leqslant n-1
\end{aligned}\qquad(12.19)$$

не должна быть равной $\gamma_1\gamma_2\ldots\gamma_m$. Словари, удовлетворяющие этому условию, называются *префиксными кодовыми* словарями[1].

Это условие можно было бы слегка ослабить без ослабления синхронизируемости словаря. Если, в частности, ни на одну из l m-последовательностей

$$\begin{aligned}
&\alpha_{i+1}\alpha_{i+2}\cdots\alpha_{i+m}, && n-l\leqslant i\leqslant n-m;\\
&\alpha_{i+1}\cdots\alpha_n\gamma_1\cdots\gamma_{i+m-n}, && n-m+1\leqslant i\leqslant n-1
\end{aligned}\qquad(12.20)$$

не наложено ограничение, то первая m-последовательность $\gamma_1\gamma_2\ldots\gamma_m$ могла бы предшествовать префиксу слова, но не более чем, на l символов, в то время как первая такая m-последовательность не могла бы появиться после правильного префикса до тех пор, пока не были бы получены, по крайней мере, $n-l+m$ дополнительных символов, следующих за префиксом. Правильный префикс мог бы, следовательно, быть опознан, если $l<n-l+m$ или $l<(n+m)/2$. Впоследствии мы сделаем ряд замечаний по поводу

---

[1] Следует различать префиксные кодовые словари и словари, обладающие свойством префикса (гл. 10). В силу того что префиксные коды представляют собой класс (в строгом смысле) блоковых кодов, то, очевидно, они обладают свойством префикса. *(Прим. авт.)*.

модифицированных префиксных кодовых словарей, удовлетворяющих этому ослабленному условию.

Заметим, что как префиксный, так и модифицированный префиксный кодовые словари являются словарями без запятой со словами из $(n+m)$ символов. Это следует из того, что каждое кодовое слово начинается одной и той же m-последовательностью и никакой стык кодовых слов не может обладать этим свойством. (Или, в случае модифицированных префиксных кодов, каждое кодовое слово должно начинаться одной и той же m-последовательностью, которая не может появиться вновь в кодовом слове до тех пор, пока не будут приняты, по крайней мере $(m+n)/2$ символов. Очевидно, что никакой стык кодовых слов не будет обладать этим свойством.) В силу того что как префиксные коды, так и модифицированные префиксные коды являются кодами без запятой при некотором дополнительном ограничении (состоящем в том, что для установления синхронизации необходимо рассмотреть лишь m символов одновременно), следует ожидать, что словари будут содержать чуть меньше слов, чем $N(n+m, r)$ из (12.3). Однако в этом случае асимптотически с ростом длины слова число слов префиксного кода имеет тот же порядок величины, что и $N(n+m, r)$, в противоположность тому, что было для кодовых словарей без запятой с инвариантными путями, рассмотренных в предыдущем параграфе. К сожалению, хотя префиксные коды легче использовать для синхронизации, чем обычные коды без запятой, они не имеют тех преимуществ при кодировании и декодировании, которые были свойственны кодам с инвариантными путями.

Можно вывести производящую функцию числа слов в максимальном префиксном кодовом словаре. Для этого введем следующие определения:

1. Префикс из m символов будет называться *повторяющимся с периодом* ν $(0<\nu\leqslant m)$, если $\gamma_1\gamma_2\ldots\gamma_\nu\ \gamma_1\gamma_2\ldots\gamma_{m-\nu}=\gamma_1\gamma_2\ldots\gamma_m$. (Заметим, что все префиксы длины m являются повторяющимися с периодом m. Следует подчеркнуть различие между повторяющимися последовательностями и периодическими последовательностями. Все периодические последовательности являются повторяющимися, но не наоборот. Непериодическая последовательность 101, например, является повторяющейся с периодом два.)

2. Говорят, что i-последовательность $\alpha_1\alpha_2\ldots\alpha_i$ будет *хорошо оканчивающейся* по отношению к некоторому префиксу $\gamma_1\gamma_2\ldots\gamma_m$, если последовательность $\gamma_1\gamma_2\gamma_3\ldots\gamma_m\alpha_1\alpha_2\ldots\alpha_i$ не имеет в качестве суффикса последовательность $\gamma_1\gamma_2\ldots\gamma_\nu$, где ν — некоторый период повторения для этого префикса.

Теорема 12.6. Пусть $\gamma_1\gamma_2\ldots\gamma_m$ является префиксом слов длины $(n+m)$ из алфавита, содержащего r символов, принадлежащих максимальному префиксному словарю $D_m(n)$, и пусть этот префикс имеет периоды повторения $\nu_1, \nu_2,\ldots, \nu_l, \nu_{i+1}\triangleq m$. Положим

$$\Delta_i \triangleq \begin{cases}1,\ i=0 \text{ или } i=\nu_j \text{ для некоторого } j,\ 1\leqslant j\leqslant l+1;\\ 0,\ \text{ для всех остальных } i\leqslant m.\end{cases}$$

Пусть $d_i = r\Delta_{i-1} - \Delta_i$ и пусть V_i обозначает число i-последовательностей, хорошо оканчивающихся по отношению к $\gamma_1\gamma_2\ldots\gamma_m$. Тогда число $N_m(n)$ слов в словаре $D_m(n)$ для всех $n \geqslant 1$ равно коэффициенту при x^n в производящей функции

$$G(x) = \left[(1 - rx)\sum_{i=1}^{m-1} V_i\, x^i + V_m\, x^m\right] \Big/ \left[1 - \sum_{i=1}^{m} d_i\, x^i\right]. \tag{12.21}$$

Доказательство. Рассмотрим $(2m+n-1)$-последовательность

$$\gamma_1\gamma_2\ldots\gamma_m\alpha_1\alpha_2\ldots\alpha_n\gamma_1\ldots\gamma_{m-1}\,. \tag{12.22}$$

Если $\alpha_1\alpha_2\ldots\alpha_n$ — хорошо оканчивающаяся, то должно существовать некоторое наибольшее целое k, $0 \leqslant k < n$, такое, что либо $\gamma_{k+1}\gamma_{k+2}\ldots\gamma_m\alpha_1\alpha_2\ldots\alpha_k = \gamma_1\gamma_2\ldots\gamma_m$, $k < m$, либо $\alpha_{k-m+1}\alpha_{k-m+2}\ldots\alpha_k = \gamma_1\gamma_2\ldots\gamma_m$, $k \geqslant m$.

Заметим, что если $k < m$, то k должно быть периодом повторения для префикса $\gamma_1\gamma_2\ldots\gamma_m$, т. е. $\Delta_k = 1$. Тогда $(n-k+m)$-последовательность, начинающаяся символом γ_{k+1} (если $k < m$) или α_{k-m+1} (если $k \geqslant m$) и оканчивающаяся символом α_n, должна быть словом из $D_m(n-k)$. Следовательно, для каждого слова из $D_m(n-k)$, $k < m$, существует единственная $(2m+n-1)$-последовательность вида (12.22), где $\alpha_1\alpha_2\ldots\alpha_n$ хорошо оканчивающаяся n-последовательность тогда и только тогда, когда $\Delta_k = 1$. Если $k \geqslant m$, то существует точно r^{k-m} таких $(2m+n-1)$-последовательностей для каждого слова из $D_m(n-k)$, так как символы $\alpha_1\alpha_2\ldots\alpha_{k-m}$ являются при этом произвольными. Таким образом,

$$\sum_{k=0}^{n-1} \Delta_k N_m(n-k) = V_n, \tag{12.23}$$

где $\Delta_k \triangleq r^{k-m}, \quad k \geqslant m.$

Далее если $n > m$ и если $\alpha_{n-m+1}\alpha_{m-n+2}\ldots\alpha_n$ хорошо оканчивающаяся последовательность, то такой же будет $\alpha_1\alpha_2\ldots\alpha_n$ и наоборот. Таким образом, $V_n = r^{n-m}V_m$ для $n > m$.

Умножая обе части равенства (12.23) на x^n и суммируя по n, получим

$$\sum_{n=1}^{\infty}\sum_{k=0}^{n-1} \Delta_k N_m(n-k)\, x^n = \sum_{k=0}^{\infty} \Delta_k\, x^k \sum_{n=k+1}^{\infty} N_m(n-k)\, x^{n-k} =$$

$$= \sum_{k=0}^{\infty} \Delta_k\, x^k \sum_{l=1}^{\infty} N_m(l)\, x^l = \sum_{n=1}^{\infty} V_n\, x^n\,. \tag{12.24}$$

Таким образом,

$$G(x) \triangleq \sum_{n=i}^{\infty} N_m(n)\, x^n = \frac{\sum\limits_{n=1}^{\infty} V_n\, x^n}{\sum\limits_{n=0}^{\infty} \Delta_n\, x^n} = \frac{\sum\limits_{n=1}^{m-1} V_n\, x^n + V_m\, x^m/(1 - rx)}{\sum\limits_{n=0}^{m-1} \Delta_n\, x^n + x^m/(1 - rx)}$$

и, умножая числитель и знаменатель выражения, стоящего в правой части, на $1-rx$, получим искомый результат. ■

Следствие. Число слов $N_m(n)$ в максимальном префиксном словаре $D_m(n)$ задается рекуррентным соотношением

$$N_m(n)=\sum_{i=1}^{m} d_i N_m(n-i) \tag{12.25}$$

для всех $n>m$.

Доказательство. Этот результат получается непосредственно, если умножить обе части равенства (12.24) на $1-\sum\limits_{i=1}^{m} d_i x^i$ и приравнять коэффициенты при x^n. ■

Например, предположим, что префиксом является 1010 и $r=2$. Так как $\gamma_1\gamma_2=\gamma_3\gamma_4$, то префикс является повторяющимся с периодом два. В силу того что он является единственным периодом повторения, $\Delta_0=1$, $\Delta_1=0$, $\Delta_2=1$, $\Delta_3=0$, $\Delta_4=1$ и

$$N_4(n)=2N_4(n-1)-N_4(n-2)+2N_4(n-3)-N_4(n-4).$$

Далее, как легко проверить, $V_1=2$, $V_2=3$, $V_3=6$, $V_4=12$ и, следовательно, из ф-лы (12.23) или из (12.21) получаем, что $N_4(1)=2$, $N_4(2)=3$, $N_4(3)=4$ и $N_4(4)=9$.

В то время как ур-ние (12.25) полезно при определении числа слов $N_m(n)$ в максимальных префиксных словарях для большинства интересных на практике длин слов $n+m$, производящая функция наиболее полезна при определении асимптотического поведения $N_m(n)$. Чтобы найти асимптотическое выражение для $N_m(n)$, фактически необходимо лишь найти наименьший по модулю корень (или корни) знаменателя $D(x)$ дроби $G(x)$. Это утверждение легко проверить, производя разложение на элементарные дроби $G(x)$ с помощью корней x_i его знаменателя. При этом типичным членом такого разложения будет

$$\frac{A_i}{x-x_i}=-\frac{A_i}{x_i\left(1-\frac{x}{x_i}\right)}=-\frac{A_i}{x_i}\left(1+\frac{x}{x_i}+\frac{x^2}{x_i^2}+\dots\right), \tag{12.26}$$

и коэффициент при x^n в многочлене $G(x)$ имеет вид: $-\sum\limits_{i}(A_i/x_i^{n+1})$.

(То же заключение справедливо и тогда, когда некоторые из корней являются кратными.) Асимптотически, следовательно, при $n\to\infty$ этот коэффициент будет абсолютно подавлен членами, которые соответствуют минимальному по модулю корню или корням.

В качестве примера использования производящей функции для отыскания асимптотического поведения $N_m(n)$ рассмотрим дробь $G(x)$, когда префикс не имеет периодов повторения (т. е. когда $\Delta_i=0$, $i\neq 0$; каждый из префиксов *aa...ab*, *aa...abb*, *aa...abbb*,...,*abb...b* обладает этим свойством). Ясно, что все n-последовательности будут хорошо оканчивающимися по отношению к неповторяющемуся префиксу при $1\leqslant n<m$, кроме самого префикса, представляющего

собой m-последовательность, когда $n=m$. Таким образом, $V_n=r^n$, $1\leqslant n<m$, $V_m=r^m-1$ и из ф-лы (12.21) имеем

$$G(x)=1/(1-rx+x^m)-1. \qquad (12.27)$$

Значения всех корней знаменателя $D(x)$ дроби $G(x)$ легко найти с помощью метода корневого годографа. Рассмотрим уравнение $K/x(x^{m-1}-r)=-1$. При $K\to 0$ точки $x=x_i$, для которых это уравнение имеет решение, стремятся к корням уравнения $x(x^{m-1}-r)=0$, т. е. стремятся к точке $x=0$ и к $(m-1)$ равноудаленным точкам $x=r^{1/(m-1)}\,e^{2\pi i[k+(1/2)]/m}$, $k=0, 1,\ldots, m-1$. Корневой годограф, показанный на рис. 12.1, при $m=10$ типичен для всех m. С увеличением K корень $x=0$ и корень $x=r^{1/(m-1)}$ стремятся друг к другу по действительной оси, в конце концов, встречаются и расщепляются на два комплексно-сопряженных числа. Модули других $m-2$ корней монотонно возрастают вместе с K и, следовательно, по меньшей мере, равны $r^{1/(m-1)}$ для всех K.

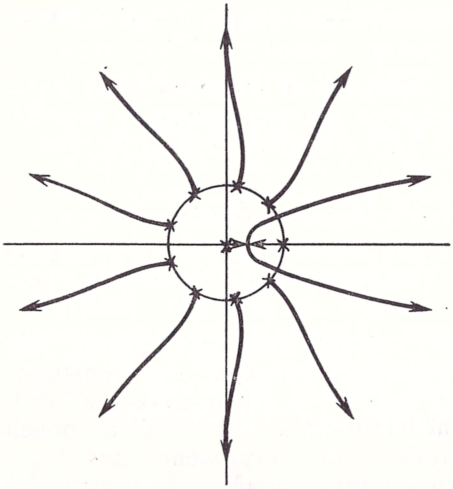


Рис. 12.1. Геометрическое место точек корней

Интересная ситуация возникает, когда $K=1$. На основе предыдущего получаем, что $D(x)$ имеет либо два положительных действительных корня, либо ни одного. Но так как $D(1/r)>0$ и $D\{m/(m-1)r\}=-[1/(m-1)][1-m^m/(m-1)^{m-1}r^m]<0$ для $m\geqslant 3$, то $D(x)$ имеет действительный корень x_0, где $(1/r)<x_0<[m/(m-1)]\times\times(1/r)$. Другой положительный действительный корень должен быть равен некоторому числу $x_1\geqslant 1$. Это становится ясным, если представить $D(x)$ в виде $(x-x_0)(x-x_1)f(x)$, когда m четное, или $(x-x_0)(x-x_1)(x-x_2)f(x)$, когда m нечетное, где $f(x)$ — многочлен, имеющий все невещественные корни $D(x)$. [Если m нечетное, то имеется вдобавок к двум положительным действительным корням отрицательный действительный корень x_2 функции $D(x)$.] Так как корни $f(x)$ должны появляться в виде комплексно-сопряженных пар, то $f(1)>0$, а так как $D(1)\leqslant 0$ и $x_0<1$, то $x_1\geqslant 1$.

Таким образом, установлено, что $D(x)$ имеет только один корень x_0, по модулю меньший единицы. Как следствие, показано, что не только $N_m(n)$ стремится к A_0/x_0^{n+1} при $n\to\infty$ [см. (12.26)], но и что входящие в $N_m(n)$ члены, которые отбрасываются, асимптотически равны нулю. (Исключение может составлять член, соответствующий возможному корню $x=1$. В любом случае влияние этого члена пренебрежимо мало.) Более того, так как x_0 — простой корень, то $A_0=\lim\limits_{x\to x_0}(x-x_0)G(x)=N(x_0)/D'(x_0)$, где $N(x)$ является числителем $G(x)$, а $D'(x)$ — производная его знаменателя.

Для того чтобы закончить вывод асимптотического выражения для $N_m(n)$, следует, однако, уточнить нашу оценку положения корня x_0. С этой целью положим $y_0=1-(1/rx_0)$. Поэтому $D(x_0)=0$ тогда и только тогда, когда $y_0[1-(m-1)y_0]<y_0(1-y_0)^{m-1}=r^{-m}<y_0$. Отсюда сразу же следует, что $y_0=r^{-m}+0(mr^{-2m})$ и

$$x_0^{-1}=r[1-r^{-m}+0(m\,r^{-2m})]. \qquad (12.28)$$

Таким образом, когда префикс не имеет периодов повторения, меньших, чем m, получаем

$$N_m(n)\sim-\frac{N(x_0)}{D'(x_0)}\,\frac{1}{x_0^{n+1}}=\frac{1}{r-m\,x_0^{m-1}}\,\frac{1}{x_0^{n+1}}, \qquad (12.29)$$

где x_0 определяется выражением (12.28).

Теорема 12.7. Асимптотически при больших длинах слов N максимальный префиксный словарь содержит, по меньшей мере, $[(r-1)r^{1/(r-1)}\log_r e]^{-1}(r^N/N)$ слов.

Доказательство. Пусть $n+m=N$ и $m=\log_r(N/c)$, где c выбрано так, чтобы m было целым. Тогда, используя ф-лы (12.28) и (12.29) и рассматривая c как постоянную, найдем, что

$$N_m(N-m)\sim\left(\frac{1}{x_0}\right)^n\sim\left(1-\frac{c}{N}\right)^N r^{N-m}\sim c\mathrm{e}^{-c}\left(\frac{r^N}{N}\right). \qquad (12.30)$$

Чтобы максимизировать это выражение при условии, что $m=\log_r(N/c)$ — целое число, заметим, что $c\mathrm{e}^{-c}$ монотонно возрастает с увеличением c при $c<1$ и монотонно убывает с ростом c при $c>1$. Далее некоторое значение c из отрезка $c_0\leqslant c\leqslant rc_0$ должно приводить к целому значению m при любом $c_0>0$. Положив $c_0\mathrm{e}^{-c_0}=rc_0\mathrm{e}^{-rc_0}$ или $c_0=(\log_e r)/(r-1)$, можно удовлетворить неравенству $c\mathrm{e}^{-c}\geqslant[(r-1)r^{1/(r-1)}\log_r \mathrm{e}]^{-1}$ для некоторого c, такого, что m — целое. Тогда асимптотически

$$\frac{1}{\mathrm{e}}\,\frac{r^N}{N}\geqslant N_m(N-m)\geqslant[(r-1)\,r^{1/(r-1)}\log_r \mathrm{e}]^{-1}\,\frac{r^N}{N}, \qquad (12.31)$$

где граница сверху справедлива в силу того, что $c\mathrm{e}^{-c}\leqslant \mathrm{e}^{-1}$. ■

Рассмотрим теперь префикс $aa\ldots a$ (т. е. префикс, имеющий все периоды повторения: 1, 2,..., m). Некоторая n-последовательность $\alpha_1\alpha_2\ldots\alpha_n$, $n\leqslant m$, будет хорошо оканчивающейся по отношению к этому префиксу тогда и только тогда, когда $\alpha_n\neq a$. В соответствии с этим $V_n=(r-1)r^{n-1}$, $1\leqslant n\leqslant m$ и из ф-лы (12.20) получаем

$$G(x)=(r-1)\,x\,(1-x)/[1-r\,x+(r-1)\,x^{m+1}]\,. \qquad (12.32)$$

Так как знаменатель $D(x)$ этой производящей функции имеет тот же вид, что и рассмотренный ранее, то могут быть использованы фактически те же самые аргументы относительно положения его корней. В частности, $D(x)$ имеет только один корень

$$x'_0=\frac{1}{r}\left(1-\frac{r-1}{r}\,\frac{1}{r^m}+O\left(\frac{m}{r^{2m}}\right)\right)^{-1} \tag{12.33}$$

с модулем, меньшим единицы. Так как этот корень меньше, чем корень x_0, найденный в предыдущем примере, то префикс *аа...а* обещает более быстрый рост $N_m(n)$ по сравнению с тем, что дает неповторяющийся префикс *аа...аb*.

На самом деле, эти два префикса соответствуют крайним значениям скорости роста $N_m(n)$. Это значит, что минимальный по модулю корень x''_0 знаменателя $D(x)$ производящей функции $G(x)$ попадает в интервал $x'_0\leqslant x''_0\leqslant x_0$, где x_0 и x'_0 задаются ф-лами (12.28) и (12.33) соответственно для всех префиксов фиксированной длины m. Чтобы проверить справедливость этого утверждения, заметим сначала, что знаменатель

$$D(x)=1-\sum_{i=1}^{m}d_i x^i=(1-rx)\sum_{i=0}^{m-1}\Delta_i x^i+x^m \tag{12.34}$$

является положительным при $x=1/r$ и отрицательным при $x=[m/(m-1)][1/r]$ (так как $\Delta_0=1$). Таким образом, многочлен $f(x)\triangleq D(x)/(1-rx)$ должен иметь корень x''_0 из интервала $1/r<x''_0<[m/(m-1)][1/r]$. Но $f(x)$ монотонно возрастает как по x, так и по коэффициентам Δ_i для всех x из этого интервала. Увеличение какого-либо Δ_i приводит, следовательно, к уменьшению x''_0. В соответствии с этим x''_0 достигает своего минимального значения (x'_0), когда $\Delta_1=\Delta_2=\ldots=\Delta_{m-1}=1$, и своего максимального значения (x_0), когда $\Delta_1=\Delta_2=\ldots=\Delta_{m-1}=0$.

В силу иронии, несмотря на то, что префикс *аа...а* гарантирует наибольшую скорость роста объема словаря для заданного значения m, всегда можно [по крайней мере, когда $r=2$] найти словарь большего объема, имеющий ту же самую длину слов $(n+m)$ и использующий префикс *аа...аb* (или какой-либо другой неповторяющийся префикс), который соответствует наименьшей скорости роста. Разрешение этого парадокса состоит в том, что значение m в этих двух случаях не будет одним и тем же. На самом деле, оптимальная длина префикса в последнем случае будет всегда больше, чем в первом. Причина этого очевидна. В любом кодовом слове за префиксом 111...1 из m символов должен всегда следовать 0, чтобы не принять за префикс также m-последовательность, начинающуюся вторым символом слова. Любое слово тем самым фактически должно начинаться префиксом 11...10 длины $(m+1)$. Тот же самый словарь оказался синхронизируемым с помощью этого нового префикса, а не первоначального. Но если используется этот префикс, то теперь в словарь могут быть включены некоторые добавочные слова и, в частности, те, которые оканчиваются серией из одной или большего числа единиц. Таким образом, для того же самого N объем словаря может быть увеличен с помощью перехода от префикса 111...1 длины m к префиксу 111...10 длины $m+1$.

Прежде чем закончить этот параграф, сделаем ряд кратких замечаний относительно объема словаря в случае, когда ограничение на префиксный код слегка ослабляется, что приводит к ранее упомянутым модифицированным префиксным кодам. Модифицированными префиксными кодами, напомним, являются коды, в которых все слова из N символов имеют один и тот же префикс длины m символов и составлены так, что этот префикс не может появиться как какая-либо m-последовательность, начинающаяся i-м символом при любом i из интервала $2 \leqslant i \leqslant [(N/2)+1]$. Если был опознан правильный префикс, то другой префикс не появится до тех пор, пока не будут приняты, по меньшей мере, $[(N/2)+1]$ символов. Если префикс обнаружен в любом другом месте, то второй префикс всегда будет обнаружен еще до того, как пройдут $[(N/2)+1]$ символов. Таким образом, установление синхронизации лишь немного сложнее, чем это было ранее, а число кодовых слов может быть увеличено. Один из методов построения такого словаря состоит в присоединении в качестве суффиксов к каждому слову из обычного словаря префиксного кода длины $m+[(n+m)/2]$ всех возможных $[(n-m+1)/2]$-последовательностей. Очевидно, что ни одна из m-последовательностей, начинающихся i-м символом любого слова из результирующего словаря, не будет совпадать с используемым префиксом при любом i из интервала $2 \leqslant i \leqslant m+[(n+m)/2]-(m-1) = [(N/2)+1]$, что и требовалось. Это построение для некоторых префиксов приводит к чрезмерным ограничениям, так как оно может наложить не являющиеся необходимыми ограничения на те m-последовательности, которые начинаются с $[(N/2)+2]$-го по $[(N/2)+m]$-й символы. Тем не менее в соответствии с ф-лой (12.30) это построение приводит к

$$N_m\left(\left[\frac{N}{2}\right]\right) r^{\{[(N+1)/2]-m\}} \sim 2ce^{-c}\left(\frac{r^N}{N}\right) \tag{12.35}$$

кодовым словам. За счет модификации асимптотически удваивается объем словаря. Интересно отметить, что здесь верхняя граница, которая получается при приравнивании c к 1, в точности совпадает с нижней границей (12.7), которая достигается для непрефиксной конструкции из § 12.2.

В этом параграфе было показано, что асимптотически в префиксном кодовом словаре содержится столько же слов, сколько и в обычном словаре без запятой с той же самой длиной слова [ср. (12.3) и (12.31)]. Как было сказано ранее, основное преимущество префиксных кодов состоит в относительной легкости, с которой они могут быть синхронизированы. Если словарь является просто словарем без запятой, необходимо рассматривать последовательности из N символов для определения того, было ли принято какое-либо кодовое слово, и проделывать это для всех N возможных начальных позиций. В противоположность этому для префиксных кодов нужно лишь рассмотреть последовательные m-последовательности $(m \sim \log_r N)$ и для получения синхронизации опознать местонахождение префикса. К сожалению, процедуры кодирования и декодирования при использовании префиксных кодов могут оказаться столь же сложными, как и в случае использования кодов без запятой. В следующем параграфе исследован другой класс синхронизируемых блоковых кодов, в котором эта трудность во многих отношениях обходится.

12.5. Коды с запятой

Другим методом установления синхронизации слов является периодическая передача *запятой* или специальной последовательности длины m для определения правильной синхронизационной позиции. Запятая называется *сингулярной* по отношению к словарю D, если она может появиться в последовательности слов из D только там, где она намеренно поставлена; в этих условиях D будет называться словарем *кода с запятой*. Таким образом, для того, чтобы запятая была сингулярной, все m-последовательности, состоящие из стыка двух кодовых слов, кодового слова и запятой или запятой и кодового слова, должны быть отличны от запятой. В модифицированном коде с запятой можно было бы допустить, чтобы запятой был только стык кодового слова и запятой, но не стык запятой и кодового слова (или наоборот).

Сингулярная запятая может передаваться всегда, когда возникает потребность в синхронизационной информации. Как только приемник опознает запятую, синхронизация устанавливается. Нет необходимости передавать запятую вновь до тех пор, пока что-либо не вызовет потерю синхронизма, так как длина слова здесь, так же как и в других параграфах этой главы, считается одинаковой для всех слов. Однако в типичных случаях запятая периодически передается через умеренно короткие интервалы после каждых k информационных слов, для того чтобы гарантировать, что в случае потери синхронизации прошло не очень много времени до того, как она вновь будет установлена.

Если $k=1$, то коды с запятой представляют собой просто префиксные коды предыдущего параграфа. Если $k>1$, то возникает новая ситуация. Теперь нужно ввести дальнейшие ограничения на кодовые слова для того, чтобы m-последовательность, образованная стыком любых двух из них, не была запятой; сама запятая не разделяет каждую пару n-последовательностей, как было в случае префиксных кодов.

Эти коды будут менее эффективны (будут более избыточны), чем префиксные коды. Так, если $N=nk+m$, то код с запятой будет сравним с префиксным кодом, имеющим тот же самый префикс длины m символов и длину слова, равную N. Очевидно, никакая N-последовательность, не принадлежащая префиксному коду, не может являться последовательностью слов кода с запятой. Некоторые N-последовательности префиксного кода могут, однако, не быть какой-либо последовательностью слов кода с запятой. Например, ни одна из этих последних последовательностей не может оканчиваться i-последовательностью, которая является началом запятой, если существует также какое-то слово, которое имеет в качестве префикса последние $m-i$ символов запятой.

Вместе с тем эти коды могут быть проще в реализации. Более того, ограничения на код не зависят от k (при $k \geqslant (m+n-1)/n$), так что частота, с которой передается запятая, может меняться в соответствии с требованиями системы без сколько-нибудь значительного изменения кодирующей и декодирующей аппаратуры.

Структура кодовых слов, конечно, будет зависеть от значений m и n. Хотя можно получить результаты для всех соотношений между m и n, ограничимся тремя наиболее интересными случаями.

Теорема 12.8. Максимальный словарь кода с запятой из r-символьного алфавита в случае, когда запятая имеет длину m, а кодовые слова длину n, содержит $M_m(n)$ слов, где

1. $M_1(n) = (r-1)^n$;
2. $M_n(n) = r^n - r^{[n/2]} - \dfrac{r^{[(n+1)/2]}-1}{r-1}, \quad n > 1$;
3. $M_{2n}(n) = r^n - 1$.

В последних двух случаях оптимальной запятой является m-последовательность вида $aaa...ab$ (или $ba...a$), состоящая из $m-1$ повторений одного из r символов a, за которыми следует некоторый другой символ $b \neq a$ или ее обращение.

Доказательство. Случай 1. $m=1$ (в качестве запятой используется лишь один символ). При этом при построении кодовых слов могут быть использованы лишь $r-1$ оставшихся символов; всего имеются $(r-1)^n$ таких слов.

Случай 2. $m=n>1$. Пусть запятой будет $\gamma_1\gamma_2...\gamma_n$. Тогда для всех i, $1 \leqslant i \leqslant n-1$ либо никакое слово из словаря не может оканчиваться i-последовательностью $s_i \triangleq \gamma_1\gamma_2...\gamma_i$, либо никакое слово не может начинаться $(n-i)$-последовательностью $p_{n-i} \triangleq \gamma_{i+1}\gamma_{i+2}...\gamma_n$. Запрещение использования s_i в качестве суффикса устраняет r^{n-i} слов из словаря, в то время как запрещение использования p_i в качестве префикса устраняет r^i слов. Предположим, что s_l является самым коротким запрещенным суффиксом. Тогда $(n-l+1)$-последовательность p_{n-l+1} не должна использоваться в качестве префикса кодового слова, и из словаря исключаются, по меньшей мере, $r^{n-l}+r^{l-1}-1$ n-последовательностей и запятая. (Вычитание единицы необходимо потому, что одна n-последовательность могла бы иметь как суффикс s_l, так и префикс p_{n-l+1}.) Но

$$r^{n-l} + r^{l-1} > r^{[n/2]} + \left\{ r^{[(n+1)/2]} - 1 \right\}/(r-1)$$

для всех $l < [n/2]$. Таким образом, самый короткий запрещенный суффикс и, по аналогии, самый короткий запрещенный префикс должны содержать, по меньшей мере, $[n/2]$ символов для того, чтобы граница $M_n(n)$ была достижимой.

Если n четное, то либо суффикс, либо префикс длины $n/2$ должны быть запрещены. Предположим, что запрещены самый короткий суффикс $s_{n/2}$ и самый короткий префикс $p_{(n/2)+1}$ (рассуждения будут такими же, если запрещены префикс $p_{n/2}$ и суффикс $s_{(n/2)+1}$). Тогда никакое кодовое слово не может иметь либо один из префиксов $p_{(n/2)+1}$ или $p_{(n/2)+2}$, либо один из суффиксов $s_{n/2}$ или $s_{(n/2)+1}$. Тогда, если $s_{n/2}$ не является суффиксом $s_{(n/2)+1}$ или $p_{(n/2)+1}$ префиксом $p_{(n/2)+2}$, различными будут все устраняемые слова, кроме, самое большее, четырех пар. Но, как легко проверить, когда $n \geqslant 8$, $r^{n/2} + 2r^{(n/2)-1} + r^{(n/2)-2} - 3$ штук n-последовательностей тем самым самоустраняются (включая саму запятую), так что число слов, допустимых для словаря, становится меньше, чем $M_n(n)$. Таким образом, для того чтобы указанная граница была достигнута, либо $s_{n/2}$ должен быть суффиксом $s_{(n/2)+1}$, либо $p_{(n/2)+1}$ должен быть префиксом $p_{(n/2)+2}$, либо и то, и другое. Но обе эти ситуации могут существовать одновременно только, если запятая состоит из одного единственного повторяемого символа $\gamma_1\gamma_2\ldots\gamma_n = aa\ldots a$. При этом ограничение на стык кодового слова и запятой, например, устранило бы все слова из словаря, имеющие односимвольный суффикс a. Одно это не дало бы возможность достичь границу $M_n(n)$. В соответствии с этим либо $s_{n/2}$ является суффиксом $s_{(n/2)+1}$ и запятая имеет вид $aa\ldots a\gamma_{(n/2)+2}\ldots\gamma_n$, либо $p_{(n/2)+1}$ является префиксом $p_{(n/2)+2}$ и запятая имеет вид $\gamma_1\gamma_2\ldots\gamma_{(n/2)-2}a\ldots a$. В первом случае все слова, имеющие либо суффикс $s_{n/2}$, либо какой-нибудь из префиксов p_{n-i}, $i=0, 1,\ldots, (n/2)-1$, будут различными. Во втором случае все слова, имеющие либо префикс $p_{(n/2)+1}$, либо какой-либо из суффиксов s_i, $i=n/2$, $(n/2)+1,\ldots, n$, будут различными. В любом из этих случаев, как легко видеть, число остающихся кандидатов для словаря ограничено величиной $M_n(n)$. Частные случаи $n=2$, 4 и 6 легко рассмотреть отдельно и показать, что для них справедлива та же самая граница.

Когда n нечетное можно использовать, по существу, те же самые рассуждения, чтобы показать, что любая запятая, приводящая к максимальному словарю, либо начинается, либо оканчивается $(n+1)/2$ повторениями одного и того же символа. (Подробный вывод оставляется читателям в качестве упражнения.) Отсюда немедленно следует указанная граница.

Рассмотрим теперь словарь $D_n(n)$, содержащий все n-последовательности, кроме тех, которые начинаются каким-либо из префиксов $p_{[n/2]+1}$, $p_{[n/2]+2}$, ..., p_n, где p_i имеет вид $aa\ldots ab$ для всех i и, кроме тех, которые заканчиваются суффиксом $s_{[(n+1)/2]} = a\ldots a$. Очевидно, что такой словарь содержит $M_n(n)$ слов. Считая, что запятая имеет вид $aa\ldots ab$, заметим, что никакой стык кодового слова и запятой, запятой и кодового слова или кодового слова и кодового слова не может образовать запятую; соответственно $D_n(n)$ является словарем кода с запятой, содержащим $M_n(n)$ слов. (То же самое доказательство, очевидно, справедливо для обращенной запятой $baa\ldots a$.)

Случай 3. $m=2n$. Если запятая представляет собой $2n$-последовательность *aaa...ab,* то нужно устранить из списка кодовых слов лишь одну n-последовательность (n-последовательность *aa...a*). Никакой стык запятой и слова или слова и запятой не может образовать запятую, и если бы какой-либо стык, включающий три слова, содержал запятую, то среднее слово непременно было бы не используемой n-последовательностью *aa...a*. Таким образом, разрешенными для словаря будут r^n-1 n-последовательностей. Независимо от соотношения между m и n, чтобы запятая была единственной, из словаря должна быть устранена, очевидно, по меньшей мере, одна n-последовательность. Следовательно, рассматриваемая запятая является оптимальной. (Опять-таки, обращение этой запятой является столь же эффективной запятой.) ■

Код с запятой при $m=2n$ является особо привлекательным с точки зрения реализации. Необходимо лишь позаботиться, чтобы было исключено сообщение, не приводящее к кодовому слову *aa...a*. Обычно это довольно легко выполнить на практике. В этом случае сообщения могут передаваться прямо с периодически вставляемой запятой. Синхронизация устанавливается всегда, когда опознается n-последовательность *aa...a*, за которой следует n-последовательность *aa...ab*.

Другие соотношения между n и m также могут иметь, по крайней мере, теоретический, если не практический интерес. Если $[m/2]<n<m$, то рассуждения, использованные для случая $m=n$, могут быть обобщены, по существу, без изменений. Тогда можно показать, что число слов в максимальном словаре с запятой

$$M_m(n) = r^n - r^{n-[(m+1)/2]} - (r^{n-[m/2]} - 1)/(r-1), \qquad (12.36)$$

$$[m/2] < n < m.$$

Вновь максимальный словарь получается, когда используется запятая *aa...b* (или *ab...bb*) и когда все префиксы вида *aa...ab* и длины $[m/2]+1$ или большей и суффикс *aa...a* длины $[(m+1)/2]$ запрещены. Аналогично, если $m\geqslant 2n$, может быть использована запятая *aa...ab* и, как и в случае $m=2n$, необходимо устранить из словаря лишь слово *aa...a*. Таким образом,

$$M_m(n) = r^n - 1, \quad n \leqslant \left[\frac{m}{2}\right]. \qquad (12.37)$$

Рассмотрение становится более сложным, однако, когда $n>m$, так как теперь запятая не должна появляться ни внутри кодового слова, ни на стыках двух или большего числа кодовых слов. Положение здесь аналогично тому, которое возникло при обсуждении префиксных кодов. Максимальное число слов в словаре легче всего определить рекуррентно.

Этот параграф закончим исследованием избыточности кодов с запятой, когда длины слов становятся большими. Для того чтобы облегчить сравнение с другими синхронизируемыми блоковыми кодами, обозначим через $N=m+kn$ полную длину, когда запятая, состоящая из m символов, должна передаваться после каждых k кодовых слов длины n символов. Множество N-последовательностей, получаемых с помощью каждого возможного последовательного соединения k слов из словаря кода с запятой и стоящей перед ними запятой, является, очевидно, словарем без запятой со «словами» из N символов. Как уже отмечалось, это множество будет более избыточным по сравнению с обычными кодами без запятой или префиксными кодами той же самой длины из-за добавочного ограничения, накладываемого на коды с запятой. Определим здесь лишь качественно, какую избыточность нужно добавить по сравнению с другими кодами, когда N велико. Для этого зафиксируем N и выберем n так, чтобы максимизировать число N-последовательностей $L_m(N)$, которые можно сформировать, используя слова длины n символов из словаря кода с запятой при трех ограничениях, представляющих наибольший интерес, а именно: $m=1$, $m=n$ и $m=2n$.

Когда $m=1$, независимо от значения n имеем $L_1(N)=(r-1)^{N-1}$. Для сравнения с границей для кода без запятой запишем это выражение в виде

$$L_1(N) = \frac{N(1-1/r)^N}{r-1}\,\frac{r^N}{N}. \tag{12.38}$$

Когда $m=n$ и n четное, получаем

$$L_n(N) = [M_n(n)]^k = \frac{r^N}{r^n}\left[1 - \frac{r}{r-1}\,\frac{an}{N}\left(1 - \frac{an}{rN}\right)\right]^{(N/n)-1} \approx$$

$$\approx \frac{r^N}{r^n}\exp\left(-\frac{r}{r-1}\,a\right), \tag{12.39}$$

где $a=a(n)=N/nr^{n/2}$ и N/n предполагается большим.

Легко убедиться в том, что как функция от n (при фиксированном N) это последнее выражение максимизируется, когда

$$1 = \frac{r}{r-1}\,a\left(\frac{\log_r e}{n} + \frac{1}{2}\right) \approx \frac{r}{r-1}\,\frac{a}{2}.$$

Таким образом, когда N (и, следовательно, n) велико, $L_n(N)$ максимизируется при

$$N = anr^{n/2} \approx 2(r-1)\,n\,r^{[(n/2)-1]}. \tag{12.40}$$

Так как для любого $\varepsilon>0$ имеем $r^{n/2}<nr^{n/2}<r^{(n/2)(1+\varepsilon)}$ при достаточно большом n, то отсюда следует, что асимптотически, когда N удовлетворяет ф-ле (12.40), $r^n \sim [rN/2(r-1)]^2$ и из (12.39) получаем

$$L_n(N) \approx \left(\frac{r-1}{r}\right)^2 \frac{4}{e^2 N}\,\frac{r^N}{N}. \tag{12.41}$$

Если n нечетное, подобные рассуждения дают

$$L_n(N) \approx r\left(\frac{r-1}{2r-1}\right)^2 \frac{4}{e^2 N}\,\frac{r^N}{N}, \tag{12.42}$$

где $N \approx [2(r-1)/(2r-1)]nr^{(n+1)/2}$. Наконец, если $m=2n$, имеем

$$L_{2n}(N) = (r^n - 1)^{(N/n)-2} = \frac{r^N}{r^{2n}}\left(1 - \frac{1}{r^n}\right)^{(N/n)-2} \approx \frac{r^N}{r^{2n}}\, e^{-a}, \qquad (12.43)$$

где $a = N/nr^n$. Это выражение максимизируется по n, когда $a \approx 2$. Следовательно, поступая, как и ранее, получаем

$$L_{2n} \approx \frac{4}{e^2 N}\, \frac{r^N}{N}. \qquad (12.44)$$

Конечно, эти асимптотические выражения справедливы только для тех N, которые связаны описанными соотношениями с n, а не для произвольных N. Здесь также можно применить метод, использованный в §12.4 для того, чтобы оценить снизу $N_m(n)$ [ср. (12.30) и (12.31)] и тем самым оценить асимптотическое значение $L_m(N)$ для всех N. Единственное отличие будет состоять в небольшом уменьшении постоянной, которая в этих выражениях умножается на r^N/N^2. В любом случае, так как здесь N было введено довольно искусственно единственно для того, чтобы была основа для сравнения с другими кодами без запятой, граница для произвольного N вряд ли является интересной.

12.6. Блоковые коды, синхронизируемые при использовании ФТ

При демодуляции r-ичного ФТ сигнала с помощью опорной несущей, получаемой непосредственно из модулированного сигнала (т. е. с помощью использования методов гл. 8 или использования относительного когерентного метода), выход детектора будет иметь r-кратную неоднозначность. Выходные символы могут быть выражены в виде $\ldots \alpha_{i-1}+\beta,\ \alpha_i+\beta,\ \alpha_{i+1}+\beta, \ldots$, где величины α известны, но где из-за отсутствия абсолютного опорного сигнала β может быть любым из r символов алфавита.

Один из методов устранения этой неоднозначности состоит в относительном кодировании информации; это означает, что информация представляется в виде разности по модулю r между последовательными символами канала, а не в виде самих символов. Этот метод имелся в виду, например, при рассмотрении ОФТ в § 4.6. Интересно отметить, что нужны лишь $N+1$ символов при использовании относительного кодирования для того, чтобы передать N символов информации. В действительности, следовательно, используется минимальное возможное число r-ичных символов (один) для устранения r-кратной неоднозначности.

В любом случае это отсутствие абсолютного опорного сигнала приводит к дополнительной трудности при синхронизации слов. Для иллюстрации рассмотрим двоичный словарь $D = \{00001, 01001, 01101, 10001, 11001, 11101\}$. Этот словарь входит в класс словарей без запятой в обычном смысле, как показано в § 12.2. Теперь, однако, из-за неопределенности опорного сигнала принимаемые слова могут быть либо из словаря D, либо из $\bar{D}$, т. е. из дополнительного к нему словаря. В отсутствие заранее установленной синхронизации поэтому последовательность ...00001000010000100..., например, может соответствовать одной из двух последовательностей слов $...w_1w_1w_1...$ или $...w_6w_6w_6...$ (где $w_1=00001$ и $w_6=11101$). Следовательно, возможная синхронизационная задержка неограничена. Очевидно, что словари, которые синхронизируемы при обычных условиях, не являются необходимо *синхронизируемыми при использовании ФТ* (т. е. синхронизируемыми, когда они используются в ФТ системе связи без абсолютного опорного сигнала).

Приведенный выше пример показывает, что, по меньшей мере, требуется наложить следующее ограничение на кодовые словари для того, чтобы они были синхронизируемыми при использовании ФТ. Если словарь D_n со словами длины n, составленными из r-ичного алфавита, содержит кодовое слово

$$w = \omega_1 \omega_2 ... \omega_n, \qquad (12.45)$$

то он не может тогда содержать никакого слова вида

$$w' = (\omega_{i+1} + \beta)(\omega_{i+2} + \beta)...(\omega_{i+n} + \beta) \qquad (12.46)$$

при любых $i=1, 2,..., n-1$ и при любом кодовом символе β ($\beta=0, 1, 2,..., r-1$). (Сложение $\omega_{i+j}+\beta$ производится по модулю r, в то время как сложение в подстрочном индексе понимается по модулю n). Это, конечно, исключает возможность того, чтобы само слово w имело вид w' для некоторого $i \neq 0$ по модулю n.

Число слов в синхронизируемом словаре при использовании ФТ может быть оценено так же, как в § 11.4, путем подсчета числа невырожденных классов эквивалентности n-последовательностей. Только теперь класс эквивалентности нужно определить иначе, включим в него все слова, связанные как w и w' [см. (12.45), (12.46)]. Это означает, что два слова принадлежат теперь одному и тому же классу эквивалентности *(классу ФТ эквивалентности)*, если одно может быть получено из другого путем циклической перестановки на некоторое число позиций и прибавления к нему постоянной n-последовательности $\beta\beta...\beta$ при любом β ($\beta=0, 1,..., r-1$). Любое слово, принадлежащее классу эквивалентности, содержащему менее чем nr различных n-последовательностей, будет называться ФТ вырожденным. Так как любое ФТ вырожденное слово может быть превращено в другое слово, из его класса эквивалентности с помощью операции того вида, который указан здесь, получаем, что справедлива следующая лемма.

Лемма 12.1. Синхронизируемый при использовании ФТ словарь может иметь самое большее одно слово из каждого невырожденного класса ФТ эквивалентности.

Теперь докажем вторую лемму, которая нужна для оценки числа слов в максимальном синхронизируемом при использовании ФТ словаре.

Лемма 12.2. Число решений k уравнения $kq=0 \pmod r$, $0\leqslant k<r$ равно (r, q), где (r, q) обозначает наибольший общий делитель целых чисел q и r.

Доказательство. Если $(r, q)=\nu$, то $r=\beta\nu$ и $q=\gamma\nu$, где β и γ — целые числа, не имеющие общих делителей, т. е. $(\beta, \gamma)=1$. Уравнение $kq=0 \pmod r$ удовлетворяется при этом тогда и только тогда, когда $k=l(\beta/\gamma)$, где l равно целому кратному γ, и, следовательно, тогда и только тогда, когда $k=\alpha\beta$ для некоторого целого α. Так как $\nu\beta=r$, то целые $k_i=i\beta<r$ дают единственные решения уравнения $kq=0 \pmod r$ для всех $i=0, 1, 2, \ldots, \nu-1$. Следовательно, имеются точно $(r, q)=\nu$ таких решений.

Теорема 12.9. Число слов в словаре, синхронизируемом при использовании ФТ и состоящем из слов длины n с символами из r символьного алфавита, не превосходит величины

$$N'(n, r)=\frac{1}{rn}\sum_{d\mid n}(r, d)\,\mu(d)\,r^{n/d},$$

где суммирование проводится по всем целым делителям n, (r, d) обозначает наибольший общий делитель r и d, а $\mu(d)$ — μ-функция Мёбиуса:

$$\mu(d)=\begin{cases}1 & \text{при } d=1;\\ (-1)^{\nu} & \text{при } d=p_1, p_2\ldots p_\nu, \text{ где } p_1, p_2, \ldots, p_\nu \text{ — различные простые числа;}\\ 0 & \text{во всех остальных случаях.}\end{cases}$$

Доказательство. Если w принадлежит ФТ вырожденному классу эквивалентности, то должно существовать некоторое наименьшее целое ν и некоторая n-последовательность $k_n\triangleq(kk\ldots k)$, $0\leqslant k<r$, такие, что $w=w^\nu+k_n$, где w^ν обозначает n-последовательность, получаемую с помощью циклического сдвига символов w на ν позиций влево. Ясно, что ν должно быть целым делителем n (ср. с леммой 11.2). Тогда также $w=(w^\nu+k_n)^\nu+k_n=w^{2\nu}+(2k)_n$ и, вообще, $w=w^{i\nu}+(ik)_n$ для любого целого i. Приравнивая первые $d=n/\nu$ символов w и $w^{i\nu}+(ik)_n$ и считая, что s обозначает произвольную ν-последовательность, получаем, что w должно иметь вид

$$w=(s, s+k_{n/d}, s+(2k)_{n/d}, \ldots, s+[(d-1)k]_{n/d}). \tag{12.47}$$

Далее, так как $w^{d\nu}+(dk)_n=w+(dk)_n=w$, то произведение dk должно равняться нулю по модулю r. Таким образом, имеются $r^{n/d}$ (n/d)-последовательностей s и (r, d) целых чисел k (лемма 12.2), представляющих различные ФТ вырожденные n-последовательности вида (12.47). Эти же самые n-последовательности являются вырожденными с периодом n/d (в смысле 11.4) тогда и только тогда, когда $k=0$ (по модулю r). Следовательно, имеются (r, d) n-последовательностей, ФТ вырожденных с минимальным периодом n/d, для каждой n-последовательности, вырожденной с тем же самым периодом в обычном смысле. Оставшаяся часть доказательства полностью аналогична доказательству теоремы 11.14; необходимо лишь подставить $(r, d)r^{n/d}$ вместо $r^{n/d}$ в доказательство теоремы 11.14, чтобы получить, что число ФТ невырожденных n-последовательностей

$$W'(n, r) = \sum_{d \mid n} (r, d)\, \mu(d)\, r^{n/d}. \tag{12.48}$$

В силу того что каждый ФТ невырожденный класс эквивалентности содержит точно nr n-последовательностей и, так как словарь, синхронизируемый при использовании ФТ, может содержать самое большее по одному слову из каждого класса эквивалентности (лемма 12.1), то теорема доказана. ■

Приведем теперь конструкцию максимальных словарей D'_n, синхронизируемых при использовании ФТ, для всех длин слов n. Пусть D_n является максимальным синхронизируемым словарем со словами длины n. (Такой словарь может быть построен методами § 11.5. Более того, если n нечетное, то D_n может в действительности быть словарем без запятой, как показано в § 12.2.) Пусть S_n — подмножество слов из D_n, сумма символов в которых равна нулю по модулю r. Например, если $r=2$ и D_5 является кодом без запятой {00001, 01001, 01101, 10001, 11001, 11101}, то $S_5=${01001, 10001, 11101}. Словарь D'_n состоит из всех слов вида

$$\begin{aligned} w &= 0,\ \sigma_1,\ \sigma_1 + \sigma_2,\ \sigma_1 + \sigma_2 + \sigma_3, \dots,\ \sigma_1 + \sigma_2 + \sigma_3 + \dots + \sigma_{n-1} = \\ &= \omega_1 \omega_2 \dots \omega_n, \end{aligned} \tag{12.49}$$

где $\sigma_1\sigma_2\dots\sigma_n$ является словом из S_n.

Теорема 12.10. Словарь D'_n является синхронизируемым при использовании ФТ.

Доказательство. Рассмотрим произвольную последовательность слов из $D'_n \dots \omega_i \omega_{i+1} \dots \omega_n \omega'_1 \omega'_2 \omega'_3 \dots \omega'_{i-1} \omega'_i \dots$. Взяв разность по модулю r между последовательными символами, получим последовательность $\dots \sigma_{i+1}\sigma_{i+2}\dots\sigma_{n-1}\sigma_n\sigma'_1\sigma'_2\dots$

[*Замечание.* Первый символ слова на выходе равен $0-(\sigma_1+\sigma_2+ + \dots + \sigma_{n-1}) = \sigma_n$ в силу того, что по построению $\sigma_1+\sigma_2+\dots+\sigma_n = 0 \pmod r$]. Так как полученная последовательность представляет собой последовательность слов из синхронизируемого словаря D_n, то она синхронизируемая. Синхронизационная задержка для D'_n лишь на один символ больше, чем аналогичная задержка для D_n в отсутствие r-кратной символьной неоднозначности. ■

Теорема 12.11. Словарь D'_n состоит из $N'(n, r)$ слов (см. теорему 12.9) и поэтому является максимальным.

Доказательство. Имеются в точности r^{n-1} n-последовательностей $\sigma_1\sigma_2\dots\sigma_n$, таких, что $\sigma_1+\sigma_2+\dots+\sigma_n=0 \pmod r$. Первые $n-1$ символов могут быть выбраны произвольно, а последний тогда определяется однозначно из соотношения $\sigma_n = -\sum^{n-1} \sigma_i$. Любая вырожденная n-последовательность (в смысле § 11.4) должна обладать тем свойством, что $w=ss\ldots s$ для некоторого $s=\sigma_1\sigma_2\ldots\sigma_{n/q}$. Число таких n-последовательностей, сумма символов которых равна нулю по модулю r равно $(r, q)r^{(n/q)-1}$, так как первые $(n/q)-1$ символов s могут быть выбраны произвольно, а последний должен быть выбран так, чтобы удовлетворялось уравнение $q(\sum_{i=}^{n/q} \sigma_i)=0 \pmod r$; согласно лемме 12.2 это уравнение имеет (r, q) решений. Так же, как и в доказательстве теоремы 11.14, нужно лишь подсчитать число тех вырожденных n-последовательностей, которые имеют период n/q, где q — произведение простых чисел, для того чтобы учесть каждую такую n-последовательность один и только один раз. В соответствии с этим имеются

$$r^{n-1} - \sum_i (r, p_i)\, r^{(n/p_i)-1} + \sum_i \sum_{j>i} (r, p_i p_j)\, r^{(n/p_i p_j)-1} + \ldots +$$
$$+ (-1)^m (r, p_1 p_2 \ldots p_m)\, r^{(n/p_1 p_2 \ldots p_m)-1} \qquad (12.50)$$

невырожденных n-последовательностей, символы которых в сумме равны нулю по модулю r. Разделив (12.50) на n, найдем, что число различных невырожденных (снова в смысле § 11.4) классов эквивалентности, имеющих слова с этим свойством, равно $N'(n, r)$. Так как каждый невырожденный класс эквивалентности дает одно слово в D_n (т. е. так как D_n — максимальный словарь), то каждый невырожденный класс эквивалентности, содержащий n-последовательности, сумма символов в которых равна нулю, дает одно слово D'_n. Таким образом, D'_n является максимальным словарем, и теорема доказана.

12.7. Заключительные замечания

В этой главе был изучен ряд ограничений, которые накладывались для того, чтобы гарантировать синхронизируемость блоковых кодовых словарей. Интересно сравнить эти различные ограничения по избыточности, которую они вносят. Пусть D будет словарем, содержащим W слов длины N из r-ичного алфавита. Тогда каждый символ содержит в среднем $(\log_2 W)/N$ бит информации. Если на D не накладывается никаких ограничений, то W равно r^N и каждый символ содержит $\log_2 r$ бит. *Избыточность* D поэтому может измеряться отношением

$$\lambda = [\log_2 r - (\log_2 W)/N]/\log_2 r = 1 - \log_r W/N. \qquad (12.51)$$

Сама по себе синхронизируемость накладывает условие $W \leqslant r^N/N$ и, следовательно, $\lambda \geqslant (\log_r N)/N$. Эта нижняя граница, на самом деле, достигается не только в классе синхронизируемых кодов, но и в классе кодов без запятой со значительно более жесткими ограничениями, как было показано в § 12.2. Префиксные коды, по крайней мере, асимптотически, так же достигают этой нижней границы (см. § 12.4). Коды без запятой с инвариантными путями из § 12.3, будучи более просто реализуемыми, имеют избыточность $\lambda \approx \frac{1}{2}[1-\log_r(r-1)]$ [ср. с (12.18)], которая в противоположность тому, что справедливо для обычных кодов без запятой, не стремится к нулю асимптотически с ростом N.

Несомненно, что кодами, имеющими наибольший практический интерес как с точки зрения реализации, так и с точки зрения синхронизации, являются коды с запятой. Если запятая помещается после каждых k слов и k выбирается подходящим образом (см. § 12.5), то получающийся словарь из «слов» длины $m+kn=N$ символов является словарем без запятой с избыточностью

$$\lambda \approx \begin{cases} (2\log_r N)/N, & m=n \text{ или } m=2n; \\ 1-\log_r(r-1), & m=1. \end{cases} \tag{12.52}$$

Таким образом, если $m=n$ или $m=2n$ (последний случай приводит к простой практической реализации), то избыточность лишь вдвое больше той, которая может быть достигнута на синхронизируемых словарях. Когда $m=1$, получающиеся коды с запятой имеют избыточность вдвое большую по сравнению с кодами без запятой с инвариантными путями. Последние, на самом деле, при больших N представляют собой, по существу, модифицированные коды с запятой для $m=1$; модификация разрешает использовать односимвольную запятую в последней половине каждого кодового слова.

Наконец, если требуется, чтобы код был синхронизируемым при использовании ФТ (§ 12.6), избыточность оценивается неравенством $\lambda \geqslant (\log_r N+1)/N$ и асимптотически совпадает с избыточностью при условии обычной синхронизируемости.

Глава 13

КОДИРОВАНИЕ ДЛЯ УСТРАНЕНИЯ ОШИБОК

13.1. Введение

Предположим, что канал связи подвержен влиянию шума, интенсивность которого достаточна, чтобы создать трудности для правильной идентификации в приемнике фактически переданных символов по сигналам, искаженным шумами. По-видимому, довольно часто будут возникать ошибки. Чтобы увеличить надежность системы, может оказаться целесообразным кодирование подлежащей передаче информации, возможно, путем передачи, помимо информационных символов, еще некоторых символов, которые дадут возможность проверить верность информационных символов. Наиболее просто посылать каждый информационный символ два раза. Если два соответствующих принимаемых символа совпадают, то к этой части сообщения возникает большее доверие, чем если бы символ передавался один раз. Если, напротив, принимаемые символы различны, то, по крайней мере, один из них должен быть ошибочным и решение относительно переданного символа может быть соответственно обесценено.

Декодер для этого кода с одним повторением мог бы работать в режиме *обнаружения ошибок*. Если какой-либо один из этой пары символов, соответствующей одному информационному символу, является ошибочным, то декодер может обнаружить это событие и сообщить потребителю о своей неспособности принять решение. Если произойдет двойная ошибка (т. е. если оба повторенных символа ошибочно определены на приемнике), то будет иметь место необнаруженная ошибка, но это событие, как мы надеемся, имеет много меньшую вероятность.

Рассмотрим теперь ситуацию, когда символ повторяется не один раз, а дважды. Тогда декодер может принять в качестве правильного символа тот, который он определяет чаще. Это означает, что если в последовательности трех выходов приемника символ s_1 возникает дважды (или три раза), а символ s_2 — один раз (или ни разу), то приемник считает, что в действительности был передан s_1 (и повторен дважды). В силу того что принять два или три последовательных ошибочных решения, по-видимому, неправдоподобно, вероятность ошибочного решения тем самым снижается. При этом, если при передаче трех символов происходит лишь одна ошибка, то будет вынесено правильное решение, и говорят, что приемник работает в режиме *исправления ошибок*.

Для того чтобы сделать предыдущие рассуждения более конкретными, предположим, что имеются лишь два символа канала и что вероятность неправильного приема для каждого из них равна p. (Конечно, эти две вероятности ошибок не обязательно должны быть равными, но очень часто они равны друг другу.) Далее предположим, что все ошибки в символах представляют собой статистически независимые события. Тогда, если используются только что рассмотренные код и алгоритм декодирования, вероятность правильного решения равна $P'_c=1-3p^2(1-p)-p^3$. Она больше, чем вероятность $P_c=1-p$ правильного решения, когда символ передается лишь один раз при $0<p<1/2$; это значит, что сказанное справедливо всегда, когда неправильный прием символа менее вероятен, чем правильный.

В случае кода с одним повторением и декодера с обнаружением ошибок вероятность неправильного решения равна p^2, что, очевидно, меньше, чем соответствующая вероятность в отсутствие повторения для всех $0<p<1$. Вместе с тем вероятность P''_c правильного решения при использовании этого кода равна $1-2p(1-p)-p^2$, что меньше, чем $P_c=1-p$ для всех $0<p<1$. Достоинство этого кода, очевидно, состоит в способности указывать на некоторые ошибки, когда они происходят, а не в способности их исправлять.

Метод повторения можно использовать неограниченно; если символ повторяется четыре раза, то могут быть исправлены одиночные ошибки и обнаружены двойные ошибки или могут быть обнаружены одиночные, двойные и тройные ошибки. Аналогично пять повторений позволяют исправить даже две ошибки в пяти символах. Стоимость повторений очевидна: если каждый символ повторяется n раз, то каждый символ переносит лишь $1/n$-ю долю информации. Другими словами, $n-1$ из n повторяемых символов являются *избыточными;* они добавляются только для того, чтобы создать защиту от шума в канале.

Очевидно, полезную избыточность можно ввести в передаваемый сигнал способами, которые отличаются от прямого повторения. Предположим, например, что после каждого блока из k *информационных* символов передается *проверочный* символ, который определяется как сумма k предыдущих символов. (Это имеет смысл только в случае, если сумма определяется подходящим образом. Например, r символов могут быть целыми числами $0, 1, \ldots, r-1$, а сумма понимается по модулю r. Или, если r степень простого числа, то символы могут быть заданы как элементы конечного поля, а сумма определяется над этим полем.) Здесь избыточным будет только один из $k+1$ символов. Тем не менее одиночную ошибку все же можно обнаружить. Это следует из того, что если любой из $k+1$ символов принят ошибочно, то $(k+1)$-й символ не будет больше суммой предыдущих k символов и будет отмечено появление ошибки. Две или большее число ошибок могут пройти необнаруженными. Если, однако, вероятность ошибки в символе p достаточно мала так, чтобы наличие двух или большего числа ошибок в $k+1$ передачах было весьма неправдоподобным, то эта способность обнаруживать одну ошибку может быть удовлетворительной.

Концепция исправления ошибок также может быть расширена. Очевидное обобщение состоит в разделении множества k информационных символов на ряд подмножеств и передаче, кроме этих k символов, проверочного символа для каждого из этих подмножеств. Так, например, за последовательностью из трех информационных символов можно передать проверочный символ для первого и второго символов, а затем — второй проверочный символ для второго и третьего символов. (Рассмотренная выше схема повторения, между прочим, может трактоваться как передача последовательности одинаковых проверочных символов для единственного информационного символа.)

Каждая из этих процедур кодирования представляет собой пример более общего метода кодирования, т. е. отображения блоков k информационных символов в блоки $n>k$ кодовых символов, называемые *кодовыми словами.* (В дальнейшем множество кодовых слов будет называться *кодовым словарем* или более кратко *кодом.* Отношение k/n, т. е. доля информационных символов в кодовом слове, называется *скоростью передачи информации.*) Имеется множество возможных способов определения такого отображения. Один из классов образуют отображения, например, состоящие в присоединении $n-k$ проверочных символов к каждым k информационным символам. Задача состоит в определении наилучшего отображения при заданном множестве условий, где наилучшее понимается в смысле получения либо минимума вероятности ошибочного приема кодового слова, либо максимума вероятности его правильного приема. (То, что эти два критерия не обязательно совпадают, можно понять на примере обсуждавшегося выше режима обнаружения ошибок.) К сожалению, они являются довольно неудобными критериями для исследования. Более простая мера качества некоторой частной схемы кодирования следует из рассмотрения соотношения между вероятностью принять одно кодовое слово вместо другого и числом соответствующих символов, которыми отличаются эти два слова. Предположим, что d_{ij} из соответствующих символов двух кодовых слов w_i и w_j не равны друг другу (например, если $w_i=00111$ и $w_j=10100$, то $d_{ij}=3$). Очевидно, что если передается одно из этих слов, то должны произойти самое малое $d_{ij}/2$ ошибок при передаче для того, чтобы принятое слово стало «ближе» ко второму слову, чем к первоначальному (отличалось меньшим числом символов от второго слова). Вообще, если d — число символов, в которых отличаются два ближайших слова, то могут быть исправлены, по меньшей мере, $e=(d-1)/2$ ошибок путем отождествления принятой n-последовательности с ближайшим к ней словом из словаря. Аналогично всегда может быть обнаружено любое множество $d-1$ или меньшего числа ошибок.

Отметим попутно, что можно было бы исправлять некоторые ошибки и обнаруживать другие. Например, все те принимаемые слова, которые находятся в пределах расстояния e от кодового слова, можно было бы считать возникшими из этого слова, в то время как принимаемые слова, отличающиеся от всех кодовых слов на расстояние, большее e, могли бы рассматриваться как не подлежащие декодированию. Тогда, если d — расстояние между ближайшими кодовыми словами, то будет считаться, что все принимаемые слова, которые содержат, по меньшей мере, $e+1$ ошибок, но не более чем $d-e-1$ ошибок, содержат ошибки, но не будут декодироваться. Если код должен исправлять вплоть до e ошибок, а также обнаруживать все принимаемые слова, содержащие более чем e, но не более чем $t=d-e-1$ ошибок, то d должно быть, очевидно, равным, по меньшей мере, $t+e+1$.

Во всех этих случаях вероятность ошибочного декодирования связана с минимальным расстоянием d между любыми двумя кодовыми словами. Эта мера расстояния, т. е. число соответствующих символов, которыми отличаются два кодовых слова, называется *хэмминговским расстоянием*.

При последующем исследовании кодов, исправляющих ошибки и обнаруживающих ошибки, словари будут сравниваться и оцениваться с помощью связанного с ними минимального расстояния d, разделяющего любые два слова; наилучшим словарем при любых заданных параметрах n и k будет тот, для которого это минимальное расстояние d максимально. Следует указать, что наилучший словарь в этом смысле не обязательно будет наилучшим в смысле максимума вероятности правильного приема или минимума вероятности ошибочного приема. Эти меры связаны с минимальным хэмминговским расстоянием, но они не обязательно монотонно зависят от него. Впоследствии мы возвратимся к этой стороне задачи.

13.2. Линейные коды

Чтобы описать более общие конструкции для кодов, исправляющих и обнаруживающих ошибки, в кодовый словарь нужно ввести структуру. Наиболее успешно используемая структура состоит в том, что кодовые символы считаются элементами некоторого конечного поля $GF(q)$, а кодовые слова образуют векторное подпространство n-последовательностей над $GF(q)$. Такой код называется *линейным (n, k)-кодом*; n обозначает число символов в каждом кодовом слове, а k — размерность подпространства.

Слова линейного кода могут быть построены, если взять все линейные комбинации множества $\{\mathbf{g}_j\}$, состоящего из k базисных векторов (или *порождающих*), с n компонентами

$$\mathbf{w}_i = \sum_{j=1}^{k} a_{ij}\mathbf{g}_j, \tag{13.1}$$

где a_{ij} — элемент поля $GF(q)$, над которым определены кодовые слова. Словарь, порождаемый k линейно независимыми векторами, содержит q^k кодовых слов. Матрица $\mathbf{G}$ с размерами $k \times n$, строки которой являются кодовыми словами $\mathbf{g}_j$, $j=1, 2,\ldots, k$, будет называться *порождающей матрицей* линейного (n, k)-кода.

Рассмотрим, например, линейный словарь $D=\{000, 202, 122, 021, 220, 110, 012, 101, 211\}$, определяемый над троичным полем. Так как он содержит девять кодовых слов, то его размерность k равна двум ($3^2=9$). Все кодовые слова, например, являются линейными комбинациями первых двух ненулевых слов. (Заметим, что каждый линейный словарь в силу того, что он определяет векторное пространство, должен содержать нейтральный элемент, т. е. вектор, все компоненты которого равны нулю.)

Одним из основных преимуществ при ограничении класса кодов линейными является относительное удобство определения минимального хэмминговского расстояния между двумя кодовыми словами. Пусть *вес* вектора определяется как число его ненулевых компонент. Тогда минимальное хэмминговское расстояние, разделяющее любые два кодовых слова в линейном коде, равно весу ненулевого кодового слова, имеющего минимальный вес в этом словаре. Это немедленно следует из того, что хэмминговское расстояние между любыми двумя кодовыми словами $\mathbf{w}_r$ и $\mathbf{w}_s$ равно весу вектора, представляющего собой разность векторов $\mathbf{w}_r-\mathbf{w}_s$, т. е. компонента $\mathbf{w}_r-\mathbf{w}_s$ не равна нулю тогда и только тогда, когда соответствующие компоненты в $\mathbf{w}_r$ и $\mathbf{w}_s$ различны. Но так как код является линейным, то слово $\mathbf{w}_t=\mathbf{w}_r-\mathbf{w}_s$ само является словом из кодового словаря и его вес равен расстоянию между $\mathbf{w}_r$ и $\mathbf{w}_s$.

Второй причиной особого внимания к классу линейных кодов является то, что он включает в себя важный класс кодов с проверками, рассмотренный ранее. Как сейчас покажем, эти два класса кодов фактически совпадают, если концепция проверок обобщается следующим образом. Пусть $(\omega_1, \omega_2,\dots, \omega_k)$ — множество информационных символов, определенных над некоторым полем $GF(q)$, и пусть проверочные символы ω_i, $k<i\leqslant n$ определяются уравнениями $\sum\limits_{j=1}^{k}\eta_{ij}\omega_j+\omega_i=0$, где суммирование производится над $GF(q)$. Это выражение можно записать следующим образом:

$$\sum_{j=1}^{n}\eta_{ij}\,\omega_j=0, \tag{13.2}$$

где $\eta_{ij}=0$ для всех $j>k$, кроме $j=i$. Использованное ранее определение проверочного символа ограничивалось случаем, когда η_{ij} равнялось -1 (или 0) для всех $j\leqslant k$. Обобщение состоит в том, чтобы рассматривать η_{ij}, $j\leqslant k$ как любые элементы из поля $GF(q)$.

Множество ур-ний (13.2) можно представить в более удобной форме, используя матричные обозначения. Пусть вектор $\mathbf{w}= (\omega_1\omega_2\dots\omega_n)$ соответствует кодовому слову, а $\mathbf{h}_{i-k}=(\eta_{i1}\eta_{i2}\dots\eta_{in})$, $i=k+1,\ k+2,\dots,\ n$ представляют собой *$(n-k)$ проверочных вектора*. Тогда существует *проверочная матрица* $\mathbf{H}$ вида

$$\mathbf{H}=[\mathbf{A}_{n-k,\,k}\,\mathbf{I}_{n-k}], \tag{13.3}$$

где $\mathbf{A}_{n-k,\,k}$ — матрица $(n-k)\times k$, а $\mathbf{I}_{n-k}$ — единичная матрица

$(n-k)\times(n-k)$, такая, что любая строка $\mathbf{h}_i$ из $\mathbf{H}$ удовлетворяет уравнению $\mathbf{w}\mathbf{h}_i=0$ для любого $\mathbf{w}$ из кода. Обратно любая n-последовательность $\mathbf{w}$, удовлетворяющая уравнению $\mathbf{w}\mathbf{h}_i=0$ при всех $\mathbf{h}_i$ из $\mathbf{H}$, является кодовым словом. Таким образом, словарь D *кода с проверками* можно определить как множество всех векторов $\mathbf{w}$, удовлетворяющих уравнению ¹)

$$\mathbf{w}\mathbf{H}^T = \mathbf{0} \underline{\underline{\Delta}} (0, 0,\ldots, 0). \tag{13.4}$$

Доказательство эквивалентности кодов с проверками и линейных кодов легко выполнить, если заметить, что все порождающие матрицы линейных кодов комбинаторно эквивалентны (эквивалентны, быть может, с точностью до перестановки столбцов) порождающей матрице вида

$$\mathbf{G} = [\mathbf{I}_k \mathbf{B}_{k,\, n-k}], \tag{13.5}$$

где $\mathbf{I}_k$ — единичная матрица $k\times k$, а $\mathbf{B}_{k,\,n-k}$ — некоторая матрица $k\times(n-k)$. Это следует в силу того, что по определению линейный код порождается $(k\times n)$-матрицей $\mathbf{W}$, имеющей строчный ранг (и, следовательно, столбцевой ранг) k. Выражая $\mathbf{W}$ в приведенно-ступенчатой форме, получаем матрицу в форме $\mathbf{G}$. Матрица $\mathbf{G}$ порождает тот же самый код, что и $\mathbf{W}$, возможно лишь с точностью до порядка его символов (т. е. до перестановки ее столбцов). Ясно, что это не меняет расстояния между двумя любыми словами кода, так что результирующие коды обладают теми же самыми расстояниями. Коды, которые могут быть порождены матрицей вида (13.5), называются *систематическими кодами* ²). Первые k символов каждого кодового слова можно отождествить с информационными символами. Это значит, что если k информационных символов $(\alpha_1, \alpha_2,\ldots, \alpha_k) \underline{\underline{\Delta}}\, \mathbf{a}$ кодируются в слово

$$\mathbf{w} = \mathbf{a}\mathbf{G}, \tag{13.6}$$

то i-м символом кодового слова будет само α_i для всех i из интервала $1\leqslant i\leqslant k$ и все информационные символы видны явно.

После этих предварительных замечаний можно сформулировать следующую теорему.

Теорема 13.1. Любой систематический код является кодом с проверками и наоборот.

13.3. Границы для минимального расстояния между кодовыми словами

Число кодовых словарей, которые могли бы быть построены, огромно почти для любого множества параметров. Пусть нужно выбрать из q^n n-последовательностей над $GF(q)$ подмноже-

---

¹) Транспонирование матрицы обозначается здесь надстрочным индексом T. *(Прим. авт.)*.

²) Иногда используется вместо этого термин «*канонический* код», а название «систематический код» дается любому коду, который эквивалентен каноническому коду при перестановке столбцов. *(Прим. авт.)*.

ство q^k в качестве словаря. Существуют $N_1=\binom{q^n}{q^k}$ способов сделать это: число N_1 чрезвычайно велико даже при умеренных значениях n, k и q. Если представляют интерес лишь линейные коды, то все еще необходимо рассматривать $N_2=L(n, k, q)$ таких кодов, где $L(r, s, q)\triangleq(q^r-1)(q^r-q)(q^r-q^2)\ldots(q^r-q^{s-1})$ — число способов выбора множества s линейных независимых векторов r-мерного векторного пространства над $GF(q)$. [Выражение для $L(r, s, q)$ легко получить, если учесть, что первым вектором может быть любой из q^r векторов подпространства, кроме нейтрального элемента, вторым — любой из q^r-q векторов, линейно не связанных с первым, третьим — любой из q^r-q^2 векторов, который не является линейной комбинацией первых двух и т. д.) Однако число неодинаковых линейных кодов меньше, чем N_2, так как каждый из них может порождаться более чем одним способом. Но даже, если используется какой-нибудь метод, чтобы избежать вторичного рассмотрения того же самого линейного кода, все еще остаются $N_3=L(n, k, q)/L(k, k, q)$ различных кодов. Для доказательства заметим, что при заданном линейном словаре имеются $L(k, k, q)$ различных способов выбора порождающего его множества. Число $L(k, k, q)$ представляет собой кратность, с которой какой-то частный код будет порождаться, когда выбираются все N_2 различных порождающих множеств. Наконец, число конкурирующих словарей можно далее снизить, рассматривая лишь систематические коды. В силу того что каждый линейный код комбинаторно эквивалентен систематическому коду, это ограничение в действительности не устраняет какие-нибудь линейные коды, но уменьшает до некоторой степени число различных словарей, которые нужно исследовать. Так как существует $q^{(n-k)k}$ различных $[k\times(n-k)]$-матриц $\mathbf{B}_{k,\,n-k}$, которые могут быть использованы при определении порождающей матрицы для кода в виде (13.5), то существуют $N_4=q^{(n-k)k}$ различных (но не обязательно комбинаторно не эквивалентных) систематических (n, k)-кодов. Но даже N_4 очень велико для того, чтобы можно было выполнить исследование с какой-либо степенью полноты. Имеется, например, более 32 млн. различных систематических двоичных (10,5)-кодов, и это число растет очень быстро с ростом n, k и q.

Главное здесь состоит в том, чтобы подчеркнуть невозможность исследования кодов с помощью перебора и, следовательно, подчеркнуть, как важно иметь возможность оценить заданный код каким-то методом, который отличается от метода сравнения его со всеми остальными кодами с теми же самыми параметрами. В этом параграфе приведены несколько верхних границ для максимального минимального расстояния кодовых словарей. Кроме того, описан метод построения словарей, имеющих заранее заданное минимальное расстояние, и посредством этого устанавливается нижняя граница для наилучшей возможной конструкции.

Некоторые верхние границы. В последующем рассмотрении будем обозначать через $D_q(n, N, d)$ словарь, состоящий из N слов длины n, определенный над q-символьным алфавитом, любые два слова из которого разделены хэмминговским расстоянием, не меньшим d. Далее пусть $V_n(q)$ — множество всех q^n n-последовательностей, определенных над некоторым q-символьным алфавитом. Если $D_q(n, N, d)$ — линейный код, то он будет называться (n, k, d)-словарем над $GF(q)$ с $k=\log_q N$. В этом случае $V_n(q)$ будет n-мерным векторным пространством над $GF(q)$. Выражение для первой границы, которое будет выведено, является следствием из двух приводимых ниже лемм.

Лемма 13.1. Пусть D является словарем с N словами, определенными над q-символьным алфавитом, и пусть $S_\rho(\mathbf{x})$ обозначает хэмминговскую *сферу* радиуса ρ в $V_n(q)$ с центром в $\mathbf{x}$(т. е. $S_\rho(\mathbf{x})$ состоит из всех n-последовательностей, которые отличаются от $\mathbf{x}$ в ρ или менее компонентах). Тогда существует такое $\mathbf{x}$, что $S_\rho(\mathbf{x})$ содержит самое меньшее N_ρ слов из D, где

$$N_\rho = \left\{ \frac{N}{q^n} \sum_{i=0}^{\rho} \binom{n}{i} (q-1)^i \right\},$$

а символ $\{l\}$ означает наименьшее целое число, большее или равное l.

Доказательство. Пусть $N_\rho(\mathbf{x})$ — число слов из D в $S_\rho(\mathbf{x})$. Тогда, так как каждое кодовое слово $\mathbf{w}$ содержится точно в $\sum_{i=0}^{\rho} \binom{n}{i} (q-1)^i$ различных сферах радиуса ρ, то

$$\max_{\mathbf{x}\in V_n(q)} N_\rho(\mathbf{x}) \geqslant \operatorname*{ave}_{\mathbf{x}\in V_n(q)} N_\rho(\mathbf{x}) = \frac{1}{q^n} \sum_{\mathbf{x}\in V_n(q)} N_\rho(\mathbf{x}) = \frac{N}{q^n} \sum_{i=0}^{\rho} \binom{n}{i} (q-1)^i, \tag{13.7}$$

и лемма доказана.

Лемма 13.2. Если $S_\rho(x)$ содержит $M \geqslant 2$ слов, принадлежащих D, то, по меньшей мере, два из них лежат на хэмминговском расстоянии d друг от друга, где

$$d \leqslant \begin{cases} \min\left[\dfrac{M\rho}{M-1}\left(2-\dfrac{\rho}{n}\,\dfrac{q}{q-1}\right),\ 2\rho\right], & \rho \leqslant \dfrac{q-1}{q}n; \\ \dfrac{M(q-1)}{(M-1)q}n, & \rho \geqslant \dfrac{q-1}{q}n. \end{cases}$$

Доказательство. Пусть $\mathbf{A}$ будет таблицей с размерами $M\times n$, строки которой — кодовые слова из $S_\rho(\mathbf{x})$. Пусть $s_j(i)$ — число появлений символа $\alpha_j(i)$ в i-м столбце $\mathbf{A}$, где $\alpha_0(i) \triangleq x_i$ (i-я компонента $\mathbf{x}$) и где другие $\alpha_j(i)$ определены произвольно, но так, чтобы, конечно, выполнялось условие $\alpha_\mu(i) \neq \alpha_\nu(i)$, $\mu \neq \nu$. Наконец, пусть

d_{ij} — расстояние между кодовыми словами $\mathbf{w}_i$ и $\mathbf{w}_j$, а $\mathbf{I}$ — множество индексов i, таких, что $\mathbf{w}_i$ принадлежит $S_\rho(\mathbf{x})$. Тогда

$$\min_{\substack{i,\, j\in I\\ i\neq j}} M(M-1)\,d_{ij} \leqslant \sum_{\substack{i,\, j\in i\\ i\neq j}} d_{ij} = \sum_{i=1}^{n}\sum_{j=0}^{q-1} s_j(i)\,(M-s_j(i)) =$$

$$= M\sum_{i=1}^{n}\sum_{j=0}^{q-1} s_j(i) - \sum_{i=1}^{n}\sum_{j=1}^{q-1} s_j^2(i) - \sum_{i=1}^{n} s_0^2(i). \qquad (13.8)$$

Согласно неравенству Шварца имеем: $n(q-1)\sum_{i=1}^{n}\sum_{j=1}^{q-1} s_j^2(i) \geqslant \geqslant \left(\sum_{i=1}^{n}\sum_{j=1}^{q-1} s_j(i)\right)^2$ и $n\sum_{i=1}^{n} s_0^2(i) \geqslant \left(\sum_{i=1}^{n} s_0(i)\right)^2$. Но $\sum_{i=1}^{n}\sum_{j=1}^{q-1} s_j(i)$ представляет собой просто сумму расстояний между $\mathbf{x}$ и кодовыми словами из $S_\rho(\mathbf{x})$, в то время как $\sum_{i=1}^{n}\left(\sum_{j=1}^{q-1} s_j(i) + s_0(i)\right) = Mn$. Полагая $\bar{\rho} = \frac{1}{M}\sum_{i=1}^{n}\sum_{j=1}^{q-1} s_j(i)$ и замечая, что $\bar{\rho}\leqslant\rho$, получаем, что

$$\min_{\substack{i,\, j\in I\\ i\neq j}} M(M-1)\,d_{ij} \leqslant M^2\bar{\rho}\left\{2-\frac{\bar{\rho}}{n}\,\frac{q}{q-1}\right\} \leqslant$$

$$\leqslant \begin{cases} M^2\rho\left\{2-\dfrac{\rho}{n}\,\dfrac{q}{q-1}\right\}, & \rho\leqslant n\dfrac{q-1}{q};\\[2ex] M^2 n\dfrac{q-1}{q}, & \rho\geqslant n\dfrac{q-1}{q}. \end{cases} \qquad (13.9)$$

Так как d, очевидно, ограничено сверху величиной 2ρ, то это доказывает лемму. ■

Объединяя леммы 13.1 и 13.2, сразу получаем следующий результат.

Теорема 13.2. (граница Элайса). Словарь $D_q(n, N, d)$ не может существовать, если не выполняется неравенство

$$d \leqslant \min_{\rho_0\leqslant\rho\leqslant[(q-1)/q]n}\left\{\frac{N_\rho}{N_\rho-1}\,\rho\left(2-\frac{\rho}{n}\,\frac{q}{q-1}\right),\; 2\rho\right\}$$

где N_ρ — наименьшее целое число, равное или большее $\frac{N}{q^n}\sum_{i=0}^{\rho}\binom{n}{i}(q-1)^i$, и где ρ_0 — наименьшее значение ρ, для которого $N_\rho\geqslant 2$.

Следствие (граница Хэмминга). Необходимым условием для существования словаря $D=D_q(n, N, q)$ является выполнение неравенства

$$N \leqslant \begin{cases} q^n \Big/ \sum\limits_{i=0}^{(d-1)/2} \binom{n}{i} (q-1)^i, & d \text{ нечетное}, \\ q^{n-1} \Big/ \sum\limits_{i=0}^{(d/2)-1} \binom{n-1}{i} (q-1)^i & d \text{ четное}. \end{cases} \tag{13.10}$$

Следствие (граница Плоткина). Словарь $D=D_q(n, N, d)$ не может существовать, если не выполнено условие

$$d \leqslant \frac{N(q-1)}{(N-1)q} n. \tag{13.11}$$

Теорема 13.3. Если существует словарь $D=D_q(n, N, d)$, то существует словарь $D_q(n-1), \{N/q\}, d)$ [1].

Теорема 13.4 (граница Грайсмера). Если D — *линейный* (n, k, d)-словарь над $GF(q)$, то существует также линейный $(n-d, k-1, \{d/q\})$-словарь над $GF(q)$.

Доказательство. Пусть $\mathbf{G}=\{\mathbf{g}_i;\ i=1, 2,\ldots, k\}$ — множество порождающих векторов кода D; без потери общности предположим, что $\mathbf{G}$ содержит вектор $\mathbf{g}_k$ веса d. Для удобства предположим, что первые $n-d$ компонент $\mathbf{g}_k$ равны нулю. (Это, возможно, потребует перенумерации компонент.) Предположим, что $\mathbf{w}$ является ненулевым словом в D, имеющим d' ненулевых компонент среди первых $n-d$. Тогда, так как $\mathbf{w}+\alpha\mathbf{g}_k$ также принадлежит D при любом α из $GF(q)$, то D должно содержать некоторое слово, имеющее среди первых $n-d$ точно d', а среди последних d — самое большее $d-\{d/q\}$ компонент, отличных от нуля. В соответствии с этим если $\mathbf{w}\neq\alpha\mathbf{g}_k$ для какого-либо α из $GF(q)$, то $d'+d-\{d/q\}\geqslant d$ и $d'\geqslant\{d/q\}$. Пусть D' является линейным $(n-d, k-1)$-словарем, порожденным $\mathbf{G}'=\{\mathbf{g}'_i,\ i=1,\ldots, k-1\}$, где $\mathbf{g}'_i$ состоят из первых $n-d$ компонент $\mathbf{g}_i$. Очевидно, что любые два слова из D' находятся друг от друга на расстоянии, по меньшей мере, d', что и следовало доказать.

Следствие. Линейный (n, k, d)-код над $GF(q)$ существует только, если

$$n \geqslant \sum_{i=0}^{k-1} d_i, \tag{13.12}$$

где $d_0=d$ и $d_i=\{d_{i-1}/q\}$.

Последние две теоремы могут быть использованы как независимо, так и совместно с теоремой 13.2, для того чтобы оценить максимум минимального расстояния d, который можно достичь на словарях D, содержащих N слов, длины n. Как следует, например, сразу же из теоремы 13.3, существование словаря $D_q(n, N, d)$ влечет за собой существование словаря $D_q(n-t, \{N/q^t\}, d)$ при любом $t \leqslant \{\log_q N\} - 1$. Положив $t = \log_q\{N-1\}$, получаем далее, что словарь не может иметь N слов из n символьного алфавита, разделенных минимальным расстоянием d, если не выполнено условие

---

[1] Здесь и далее вновь $\{l\}$ обозначает наименьшее целое, большее или равное l. *(Прим. авт.)*.

$$d \leqslant n - \{\log_q N\} + 1. \tag{13.13}$$

В случае, по крайней мере, линейных кодов теорема 13.4 может иногда приводить к более точной границе, чем граница в теореме 13.2. Последняя граница, например, не запрещает существование словаря D_2 (10, 16, 5), но согласно теореме 13.4 никакой линейный двоичный код не может обладать этими параметрами. Аналогично двоичный линейный (15, 8, 5)-код мог бы существовать, если бы существовал (10, 7, 3)-код (ср. с теоремой 13.4). Последний код запрещен, однако, границей из теоремы 13.2, хотя запрещение не распространяется на словарь. D_2 (15, 256, 5). Таким образом, может существовать нелинейный код с этими параметрами, но не линейный[1].

Обсуждение верхних границ закончим, доказав еще два следствия теоремы 13.4.

Следствие. Линейный (n, k)-код над $GF(q)$ с расстоянием

$$d = \beta_0 q^{k-1} - \sum_{i=1}^{k-1} \beta_i q^{l_i - 1}$$

$$(\beta_i = 0, 1, 2\ldots, q-1; \quad 1 \leqslant l_{j+1} < l_j < k-1) \tag{13.14}$$

существует только в том случае, если

$$n \geqslant \beta_0 (q^k - 1)/(q-1) - \sum_{i=1}^{k-1} \beta_i (q^{l_i} - 1)/(q-1). \tag{13.15}$$

Следствие[2]. Если линейный q-ичный (n, k)-код имеет минимальное расстояние $d \leqslant q^{k-1}$, то

$$n \geqslant \frac{q}{q-1}(d-1) + k - \log_q d. \tag{13.16}$$

Нижняя граница Гилберта. Прежде чем закончить обсуждение границ, убедимся в том, что существуют линейные коды, по крайней мере, хоть с какими-то способностями к исправлению или обнаружению ошибок. Вывод границы Гилберта показывает, что можно построить q-ичные линейные (n, k)-коды с заданным минимальным расстоянием. Основания для этого построения дает следующая лемма.

---

[1] Интересно отметить, что существует-таки нелинейный код с этими параметрами. Наилучший линейный (15,8)-код имеет расстояние 4. Это один из нескольких случаев, когда известно, что существует нелинейный код, имеющий большее минимальное расстояние, чем допустимое для линейного кода с той же самой длиной слова и размерностью. *(Прим. авт.)*.

[2] Иногда эта граница также называется границей Плоткина. *(Прим. авт.)*.

Лемма 13.3. Если имеется кодовое слово с весом d, порожденное матрицей $\mathbf{G}$, то должна существовать линейная зависимость между точно d столбцами порождающей матрицы $\mathbf{H}$ нуль-пространства и наоборот.

Эта лемма является основной для конструкции Гилберта. Чтобы построить линейный (n, k)-код с минимальным расстоянием не меньшим d, нужно выбрать столбцы $(n-k)\times k$-матрицы $\mathbf{H}$ так, чтобы никакое множество из $d-1$ или меньшего их числа не было линейно зависимым. Так, первый столбец $\mathbf{h}_1$ матрицы $\mathbf{H}$ может быть любой $(n-k)$-последовательностью над $GF(q)$, кроме чисто нулевого вектора $\mathbf{O}^T$. Второй столбец $\mathbf{h}_2$ может быть любым, кроме $\mathbf{O}^T$, или (если $d>2$) $\mathbf{h}_1$, умноженного на любой из $q-1$ ненулевых элементов $GF(q)$; $\mathbf{h}_3$ может быть любым, кроме $\mathbf{O}_T$, $\mathbf{h}_1$, $\mathbf{h}_2$, умноженных на любой из $q-1$ ненулевых элементов $GF(q)$ (если $d>2$) или $(q-1)^2$ линейных комбинаций, включающих в себя как $\mathbf{h}_1$, так и $\mathbf{h}_2$ (если $d>3$). Вообще, $(j+1)$-й столбец из $\mathbf{H}$ может быть выбран и оставшихся $(n-k)$-последовательностей лишь после того, как все возможные линейные комбинации из $d-2$ или меньшего числа j ранее выбранных столбцов $\mathbf{H}$ были исключены. Это гарантирует, что никакие из $d-1$ или меньшего числа выбранных столбцов не являются линейно зависимыми. В худшем случае все эти устраненные $(n-k)$-последовательности являются различными, поэтому можно заведомо выбрать n-й столбец из $\mathbf{H}$, если после того, как все, возможно различные

$$\sum_{j=0}^{d-2}\binom{n-1}{j}(q-1)^j \triangleq N(n, q, d) \qquad (13.17)$$

$(n-k)$-последовательности были устранены, остался, по крайней мере, один столбец. Так как имеются $q^{(n-k)}$ различных $(n-k)$-последовательностей, то это возможно, если $N(n, q, d)<q^{n-k}$. Так как ранг $\mathbf{H}$ не может быть больше, чем $n-k$, то словарь должен содержать, по меньшей мере, q^k слов. Следовательно, доказана следующая теорема.

Теорема 13.5. Можно построить q-ичный линейный (n, k)-словарь с минимальным расстоянием $d\geqslant 2$ для всех n, k и d, удовлетворяющих неравенству

$$q^k < q^n \Big/ \sum_{i=0}^{d-2}\binom{n-1}{i}(q-1)^i . \qquad (13.18)$$

13.4. Циклические коды

За некоторыми важными исключениями поиск хороших конструкций линейного кода, исправляющего ошибки, оказывался успешным только после того, как были наложены еще бо́льшие ограничения на кодовую структуру. По мере того как математические ограничения, которым должен удовлетворять код, становятся более жесткими, подмножество допускаемых кодов становится, конечно, меньшим, и наилучшие коды с самого начала могут даже быть исключением из рассмотрения. Вместе с тем те коды, которые останутся, будут легче поддаваться анализу, и хорошие коды в этом ограниченном классе будет легче описать.

Ограничение, которое применяется наиболее эффективно, состоит в требовании того, чтобы линейный код был *циклическим*. Обозначим через $\mathbf{w}^i$ циклическую перестановку символов кодового слова $\mathbf{w}$ на i позиций влево [если $\mathbf{w}=w_0w_1\ldots w_{n-1}$, то $\mathbf{w}^i=(w_iw_{i+1}\ldots w_{n-1}w_0w_1\ldots w_{i-1})$]. Линейный словарь D называется циклическим тогда и только тогда, когда он вместе с каждым словом $\mathbf{w}$ из D содержит также слово $\mathbf{w}^i$ для каждого целого i. Все эти перестановки не обязательно должны быть различными. Например, каждый из словарей 0000, 1111 и 0000, 0011, 0110, 1100, 1001, 0101, 1010, 1111 является циклическим.

Послезно ассоциировать с каждым кодовым словом $\mathbf{w}=(w_0w_1\ldots w_{n-1})$ многочлен

$$w(x)=w_0+w_1x+w_2x^2+\ldots+w_{n-1}x^{n-1}. \tag{13.19}$$

Если код является циклическим, то многочлен $x^lw(x)$ также должен представлять собой кодовое слово; здесь показатель степени берется по модулю n; $x^lw(x)$ соответствует слову, которое получается с помощью циклической перестановки символов $\mathbf{w}$ на l позиций вправо (на $n-l$ позиций влево). Более того, так как код линейный, то произведение $p(x)w(x)$ представляет собой кодовое слово при любом многочлене $p(x)$ с коэффициентами, которые являются элементами поля, над которым определен код. Очевидно, что приведение по модулю n показателей степеней в многочлене $p(x)$ эквивалентно приведению многочлена по модулю многочлена x^n-1. [Если $p(x)=q(x)(x^n-1)+r(x)$, где $r(x)$ — многочлен степени, меньшей чем n, то $p(x)=r(x)$ по модулю x^n-1.]

Теорема 13.6. Каждое кодовое слово в циклическом (n, k)-коде может быть представлено многочленом вида $\alpha(x)g(x)$, где $\alpha(x)$ — многочлен степени $k-1$ или меньше в зависимости от рассматриваемого кодового слова, а $g(x)$ является нормированным [1]) делителем многочлена x^n-1, имеет степень $n-k$ и определяется единственным образом.

Многочлен $g(x)$, определенный в теореме 13.6, будет называться *порождающим многочленом* (n, k)-*кода*.

Пусть теперь многочлен $v^*(x)$ определяется как

$$v^*(x)=v_{n-1}+v_{n-2}x+v_{n-3}x^2+\ldots+v_0x^{n-1}=\sum_{i=0}^{n-1}v_{n-1-i}x^i, \tag{13.20}$$

где $(v_0v_1\ldots v_{n-1})$ — n-последовательность в нуль-пространстве рассматриваемого кода; рассмотрим произведение $w(x)v^*(x)$, в котором показатели степеней берутся по модулю n, $w(x)v^*(x)=$

---

[1]) Нормированным многочленом называется многочлен, старший коэффициент которого равен 1. (*Прим. авт.*).

$=\sum\limits_{i=0}^{n-1}(v_0w_{i+1}+v_1w_{i+2}+\ldots+v_{n-1}w_i)x^i$. Коэффициент при x^i в произведении многочленов является скалярным произведением, представляющим собой одно из проверочных соотношений, которому должен удовлетворять вектор $\mathbf{w}^{i+1}$. Следовательно, если $w(x)$ является многочленом кодового слова, а $v^*(x)$ — проверочный многочлен, определенный выше, то произведение $w(x)v^*(x)$ должно быть равным нулю, если показатели степеней приводятся по модулю n. Другими словами, произведение $w(x)v^*(x)$ должно делиться на x^n-1:

$$w(x)v^*(x)=p(x)(x^n-1). \tag{13.21}$$

Теорема 13.7. Нуль-пространство циклического кода также является циклическим кодом с порождающим многочленом $h(x)=(x^n-1)/g(x)$.

Доказательство. Очевидно, что $\alpha(x)h(x)\beta(x)g(x)=\alpha(x)\beta(x)\times(x^n-1)=p(x)(x^n-1)$ и любая n-последовательность, соответствующая какому-либо из многочленов $\alpha(x)h(x)$, находится в нуль-пространстве кода, порождаемого многочленом $g(x)$. Обратно предположим, что $v^*(x)$ соответствует некоторой n-последовательности в нуль-пространстве. Тогда $g(x)v^*(x)=p(x)(x^n-1)=p(x)g(x)h(x)$, так что

$$v^*(x)=p(x)h(x). \tag{13.22}$$

Все многочлены, представляющие n-последовательности из нуль-пространства, имеют вид (13.22) и (наоборот), где $h(x)=(x^n-1)/g(x)$, что и требовалось доказать. ■

Заметим, что пространство циклического кода, порождаемого многочленом $g(x)=\sum\limits_{i=0}^{n-k}g_ix^i$, натянуто на векторы

$$\mathbf{G}=\begin{bmatrix} g_0 & g_1 & \cdots & g_{n-k} & 0 & 0 & \ldots & 0\\ 0 & g_0 & \cdots & g_{n-k-1} & g_{n-k} & 0 & \ldots & 0\\ \vdots & \vdots & & & & & & \vdots\\ 0 & 0 & \ldots & g_0 & g_1 & g_2 & \ldots & g_{n-k}\end{bmatrix}, \tag{13.23}$$

а его нуль-пространство натянуто на векторы

$$\mathbf{H}=\begin{bmatrix} h_0 & h_1 & \ldots & h_{k-1} & h_k & 0 & \ldots & 0\\ 0 & h_0 & \ldots & h_{k-2} & h_{k-1} & h_k & \ldots & 0\\ \vdots & \vdots & & & & & & \vdots\\ 0 & 0 & \ldots & h_0 & h_1 & h_2 & \ldots & h_k\end{bmatrix}, \tag{13.24}$$

где $h(x)=\sum_{i=0}^{k} h_{k-i}x^i$ — порождающий многочлен нуль-пространства.

Более того, матрица $\mathbf{G}$ из равенства (13.23) может, очевидно, быть записана в виде (13.5) с помощью последовательности элементарных операций, выполняемых только со строками. В силу того что эти операции со строками оставляют результирующий словарь неизменным, все циклические коды являются систематическими.

Кодовое слово $\mathbf{w}=(w_0 w_1 \dots w_{n-1})$ принадлежит циклическому (n, k)-кодовому словарю тогда и только тогда, когда

$$\sum_{j=l}^{k+l} w_j h_{j-l}=\sum_{i=0}^{k} w_{i+l}\, h_i = 0 \tag{13.25}$$

для всех $l=0, 1, \dots, n-k-1$, где $\mathbf{h}=(h_0 h_1 \dots h_k 0 \dots 0)$ — n-последовательность его нуль-пространства. Это сразу же следует из выражения (13.24) для порождающей матрицы нуль-пространства. В соответствии с этим символы любого кодового слова должны удовлетворять рекуррентному соотношению

$$w_{l+k} = -\frac{1}{h_k}\sum_{i=0}^{k-1} w_{i+l}\, h_i,\; l=0, 1, \dots, n-k-1. \tag{13.26}$$

Символы w_j при всех $k \leqslant j \leqslant n-1$ однозначно определяются по первым k символам $w_0, w_1, \dots, w_{k-1}$ с помощью этого разностного уравнения.

Стандартная процедура отыскания решения линейных разностных уравнений состоит в нахождении решения в виде $w_l=x^l$ и определении корней образующегося многочлена. При этом решение задается равенством $w_l=\beta^l$, где β — любой корень многочлена

$$\sum_{i=0}^{k} h_i\, x^{i+l} = x^{l+k}\sum_{j=0}^{k} h_{k-j}\, x^{-j} = x^{l+k}\, h\left(\frac{1}{x}\right), \tag{13.27}$$

$h(x)$ было определено ранее. Корни $h(1/x)$ существуют в некотором расширении поля $GF(q)$, над которым определен код.

Один из корней многочлена (13.27), очевидно, есть $x=0$. Так как $x^k h(1/x)$ является многочленом степени k, то существуют вплоть до k других решений $w_l=\beta^l{}_i$, где $h(\beta^{-1}{}_i)=0$, и так как разностное уравнение является линейным, то любая линейная комбинация этих k решений также должна быть решением. Общее решение поэтому должно иметь вид

$$w_l = \sum_{i=1}^{k} c_i\, \beta_i^l, \tag{13.28}$$

где c_i — постоянные, которые должны быть выбраны так, чтобы удовлетворялись начальные условия:

$$w_0=\sum_{i=1}^{k} c_i;\ w_1=\sum_{i=1}^{k} c_i\beta_i;\quad w_2=\sum_{i=1}^{k} c_i\beta_i^2,\ldots,w_{k-1}=\sum_{i=1}^{k} c_i\beta_i^{k-1}.$$

Это означает, что вектор $\mathbf{c}=(c_1, c_2,\ldots, c_k)$ должен удовлетворять уравнению

$$\mathbf{M}\,\mathbf{c}^T=\widetilde{\mathbf{w}}^T, \qquad (13.29)$$

где

$$\mathbf{M}=\begin{bmatrix} 1 & 1 & \ldots & 1 \\ \beta_1 & \beta_2 & \ldots & \beta_k \\ \beta_1^2 & \beta_2^2 & \ldots & \beta_k^2 \\ \vdots & \vdots & & \vdots \\ \beta_1^{k-1} & \beta_2^{k-1} & \ldots & \beta_k^{k-1} \end{bmatrix}$$

и $\widetilde{\mathbf{w}}=(w_0, w_1,\ldots, w_{k-1})$.

Уравнение (13.29) будет иметь решение $\mathbf{c}$ тогда и только тогда, когда матрица $\mathbf{M}$ имеет ранг k, и поэтому тогда, когда определитель матрицы $\mathbf{M}$ не равен нулю. Но при всех $k>1$ имеем

$$\det\mathbf{M}=\prod_{\substack{i,\,j=1\\ i>j}}^{k}(\beta_i-\beta_j). \qquad (13.30)$$

Чтобы показать это, заметим, что обе части уравнения (13.30) являются многочленами $p(\beta_i)$ степени $k-1$ от какого-либо одного из переменных β_i [т. е. $p(\beta_i)=\sum_{j=0}^{k-1} d_j\beta^j{}_i$]. Более того, если $\beta_i=\beta_j$ для любых $j\neq i$, то $\det\mathbf{M}=0$, и поэтому $p(\beta_i)$ имеет делитель $\beta_i-\beta_j$. Так как обе части соотношения (13.30) являются многочленами одной и той же степени и имеют одни и те же делители, то они отличаются самое большее на постоянный множитель. Но поскольку коэффициент при $1\,\beta_2\beta^2{}_3\ldots\beta_k^{k-1}$ совпадает для обоих многочленов, то, на самом деле, они должны быть равными. (Этот определитель, между прочим, называется определителем Вандермонда.)

Поэтому получаем, что $\det\mathbf{M}\neq 0$, если все корни β_i различные. [Если они не являются различными, то решение все же можно получить, хотя оно и не имеет вида (13.28). Во всех представляющих для нас интерес ситуациях, однако, β_i будут различными.] Таким образом, можно записать решения относительно коэффициентов c_i так, чтобы удовлетворялись начальные условия. Так как w_l в (13.28) удовлетворяют как рекуррентным соотношениям, так и начальным условиям, то в действительности они должны быть символами кодового слова, имеющего эти k заданных информационных символов.

Фактически мы лишь указали другой способ определения символов слова циклического кода по информационным символам. Так как можно было бы сделать это значительно проще с помощью других методов, то казалось бы, что результат едва ли заслуживает затраченных усилий. Польза ур-ния (13.28), однако, станет ясной после следующих замечаний. Прежде всего, корни β_i многочлена $h(1/x)$ всегда могут быть выражены в виде $\beta_i=\beta_0\beta^{e_i}$, где e_i — целые числа, а β_0 и β — элементы некоторого поля $GF(q^m)$. (В частности, $\beta_i=\alpha^{e_i}$, где α — примитивный элемент этого поля.) Но если $\beta_i=\beta_0\beta^{e_i}$, то ур-ние (13.28) записывается в виде

$$w_l=\beta_0^l\sum_{i=1}^{k}c_i\left(\beta^{e_i}\right)^l. \tag{13.31}$$

В соответствии с этим каждое кодовое слово из словаря можно ассоциировать с многочленом

$$g_w(x)=\sum_{i=1}^{k}c_i\,x^{e_i} \tag{13.32}$$

так, что $w_l=\beta_0^l g_w(\beta^l)$. Эти многочлены в литературе по теории кодирования обычно называются *многочленами Маттсона—Соломона.*

Предположим теперь, что $\max\limits_{1<i<k} e_i=s$. Тогда $g_w(x)$ является многочленом от x степени s. Имеется самое большее s решений $x=\beta^l$, для которых $g_w(\beta^l)=0$. Если β является элементом порядка e, то, следовательно, самое меньшее $[n/e](e-s)$ величин w_i должны быть ненулевыми. Так как это справедливо для любого ненулевого кодового слова из словаря, то сам словарь должен обладать минимальным весом $d\geqslant[n/e](e-s)$. Часто этот метод удобен для оценки снизу минимального веса циклического кодового словаря. Отметим, что ни β, ни целые числа e_i не определяются однозначно соотношением $\beta_i=\beta_0\beta^{e_i}$ и s может быть различным для различных элементов β. Тем не менее нижняя граница $d\geqslant[n/e](e-s)$ справедлива для всех β, удовлетворяющих этому соотношению. Резюмируем эти результаты следующей теоремой.

Теорема 13.8. Пусть D — циклический кодовый (n, k)-словарь, нуль-пространство которого порождается многочленом $h(x)$, и пусть $h(x)$ имеет (различные) корни $\beta_1^{-1}, \beta_2^{-1},\ldots, \beta_k^{-1}$. Тогда для каждого слова $\mathrm{w}=(w_0w_1\ldots w_{n-1})$ из D существует ассоциированный многочлен Маттсона—Соломона $g_w(x)=\sum\limits_{i=1}^{k}c_ix^{e_i}$ такой, что $w_l=\beta_0^l g_w(\beta^l)$. [Целые числа e_j определяются соотношением $\beta_0\beta^{e_i}=\beta_i$, $i=1, 2,\ldots, k$, а коэффициенты c_i ур-нием (13.29).] Вес слова с минимальным весом из D ограничен неравенством $d\geqslant[n/e](e-s)$, где $s=\max\limits_{1<i<k} e_i$ и e — порядок β.

13.5. Некоторые важные циклические коды

Для того чтобы $h(x)$ порождал нуль-пространство циклического (n, k)-кода, $h(x)$ должен делить x^n-1, т. е. $(x^n-1)/h(x)$ должен быть многочленом с коэффициентами из кодового поля. Поэтому один из методов выявления всех циклических кодов, которые существуют для заданного значения n, состоит в определении всех неприводимых делителей многочлена x^n-1 над рассматриваемым полем. Например, поскольку над двоичным полем $x^7-1=(x+1)\times\times(x^3+x+1)(x^3+x^2+1)$, то существуют циклические (7, 1), (7, 3), (7, 4), (7, 6) и, конечно (7, 7)-коды. Но так как многочлены $x+1$, x^3+x+1 и x^3+x^2+1 сами неприводимые над этим полем, то не существуют никакие другие двоичные циклические коды длины семь. Эти коды легко найти. Так как (7, 1)-код соответствует многочлену $h(x)=1+x$, то кодом будет множество 0000000, 1111111. Коду (7, 3) соответствует $h(x)=x^3+x+1$, так что код имеет вид 0000000, 1110100, 1101001, 1010011, 0100111, 1001110, 0011101, 0111010.

Код (7, 4) соответствует $h(x)=(x^3+x+1)(x+1)=x^4+x^3+x^2+1$ и содержит все слова из указанного выше (7, 3)-кода, так как если многочлен $w(x)(x^3+x+1)$ равен нулю по модулю x^7-1, то это справедливо и для $w(x)(x^3+x+1)(x+1)$. Кроме того, многочлен $w(x)$, представляющий ненулевое слово из (7, 1)-кода, удовлетворяет условию $w(x)\ (x+1)=0$ по модулю x^7-1, так что $w(x)\ (x+1)(x^3+x+1)=0$ по модулю x^7-1, и вектор, состоящий из одних единиц, также является словом (7, 4)-кода. Код (7, 4) поэтому является объединением указанного выше (7, 3)-кода с его смежным классом, содержащим n-последовательность из одних единиц. Заметим, что другой (7,3)-код определяется с помощью многочлена $h(x)=(x^3+x^2+1)$, а другой (7,4)-код — с помощью многочлена $h(x)=(x^3+x^2+1)(x+1)$. Эти последние коды являются нуль-пространствами соответственно (7,4) и (7,3)-кодов, описанных выше.

Хотя этот подход и поучителен, но, очевидно, что он неудобен для больших значений n. Поэтому важно иметь возможность определить общие классы кодов, которые существуют для многих параметров n и k, и найти относящиеся к ним расстояния. Это и является задачей настоящего параграфа.

Начнем с сильно ограниченного класса кодов, в котором все слова, кроме чисто нулевого слова, имеющегося в любом словаре, являются циклическими перестановками любого из этих слов и в котором все такие перестановки являются различными. Такие коды будут называть *циклическими кодами максимальной длины*. Смысл этого названия станет ясным после следующей теоремы.

Теорема 13.9. В циклическом (n, k)-коде максимальной длины, определенном над полем $GF(q)$, длина кодовых слов n должна быть равной q^k-1.

Ясно, что для того чтобы все n циклических перестановок слова из k-мерного циклического кода были различными, n не должно быть больше q^k-1. Поэтому их называют циклическими кодами максимальной длины.

Любое слово в циклическом коде максимальной длины должно после сложения с любой из его циклических перестановок, умноженной на скаляр, давать другую циклическую перестановку самого себя. Это верно потому, что код является линейным (так что все линейные комбинации кодовых слов также являются кодовыми словами) и потому, что все ненулевые кодовые слова являются циклическими перестановками одного слова. (Отметим отличие этого кода от обычных циклических кодов. В последних все циклические перестановки каждого кодового слова являются кодовыми словами, но все кодовые слова не обязательно являются циклическими перестановками всех других слов.) В качестве примера рассмотрим двоичный (7, 3)-код, рассмотренный ранее. Этот код является циклическим кодом максимальной длины. Сумма слова 1110100 и любой из его циклических перестановок, например, 1101001 должна быть другой его циклической перестановкой; в этом случае — 0011101. Это свойство кодов иногда называют *аддитивно циклическим* свойством [1].

Теорема 13.10. Многочлен $h(x)$ порождает нуль-пространство циклического (n, k)-кода максимальной длины над полем $GF(q)$ тогда и только тогда, когда $h(x)$ — примитивный многочлен [т. е. тогда и только тогда, когда корни $h(x)$ порядка $n=q^k-1$].

Следствие. Существует циклический (q^k-1, k)-код максимальной длины для каждого $q=p^m$, где p — простое, а m — целое число, и для каждого целого k.

Расстояния в циклических кодах максимальной длины легко определяются с помощью следующей леммы.

Лемма 13.4. Пусть $\mathbf{D}$ является матрицей $q^k \times n$, а строки $\mathbf{D}$ представляют собой кодовые слова линейного кода длины n над полем $GF(q)$. Тогда любой столбец $\mathbf{D}$, имеющий хотя бы одну ненулевую компоненту, содержит каждый элемент поля точно q^{k-1} раз.

Теорема 13.11. Каждое ненулевое слово циклического кода максимальной длины содержит q^{k-1} раз каждый ненулевой элемент поля и $q^{k-1}-1$ раз — нулевой элемент. Поэтому такие коды имеют минимальный вес $d=(q-1)q^{k-1}$. В силу того что он является максимально возможным минимальным весом для (q^k-1, k)-кода в соответствии с границей (13.11), эти коды являются оптимальными.

Следующие кодовые слова, объединенные со всеми их циклическими перестановками и n-последовательностью из одних нулей, дают примеры циклических кодов максимальной длины:

---

[1] То, что все слова двоичного кода максимальной длины являются циклическими перестановками последовательности линейного регистра сдвига с обратной связью (см. § 6.7) будет (если это еще не стало очевидным) вскоре показано. (*Прим. авт.*).

$(n=1,\quad k=1,\quad q=2)$: 1
$(n=2,\quad k=1,\quad q=3)$: 21
$(n=4,\quad k=1,\quad q=5)$: 2431
$(n=3,\quad k=2,\quad q=2)$: 110
$(n=7,\quad k=3,\quad q=2)$: 1110100
$(n=15,\quad k=4,\quad q=2)$: 100110101111000
$(n=8,\quad k=2,\quad q=3)$: 11202210
$(n=26,\quad k=3,\quad q=3)$: 20212210222001012112011100

Каждое ненулевое слово циклического кода максимальной длины имеет ряд свойств, которые характерны для чисто случайной q-ичной последовательности. Поэтому эти n-последовательности часто называются *псевдослучайными* или *псевдошумовыми* последовательностями.

Имея в виду рассмотрение, проведенное в § 13.4, не следует удивляться, что циклические коды иногда более удобно описывать с помощью корней порождающих их многочленов. Наибольший и самый важный класс циклических кодов, обычно называемых БЧХ кодами, определяется именно таким образом. (Буквы БЧХ составляют начальные буквы фамилий Боуза, Чоудхури и Хоквингема, которые впервые описали конструкцию и свойства этих кодов.)

Теорема 13.12. Пусть β — элемент порядка n в поле $GF(q^m)$ и пусть $g(x)$ — многочлен наименьшей степени с коэффициентами из $GF(q)$, имеющий корни β^{m_0}, β^{m_0+1}, β^{m_0+2}, …, β^{m_0+t-1}. Тогда $g(x)$ порождает циклический (n, k)-код над $GF(q)$ для некоторого $k \geqslant 0$ с минимальным расстоянием, по меньшей мере, равным $d=t+1$.

Коды этой теоремы и есть БЧХ коды. Заметим, что длина слова n должна быть делителем числа q^m-1 при некотором целом m. Это соотношение определяет наименьшее поле $GF(q^m)$, содержащее β, т. е. m — наименьшее целое число, для которого $q^m=1$ по модулю n.

Наиболее важными классами БЧХ кодов являются те, которые получаются при $m_0=0$ и при $m_0=1$. Размерность k легко оценить снизу для каждого из этих случаев. Пусть $m_i(x)$ — многочлен наименьшей степени над полем $GF(q)$, имеющий корень β^i. Тогда элементы β^{iq^j} также являются корнями $m_i(x)$ при всех $j=1, 2, \ldots, m$. Так как каждый корень вида β^r, где r делится на q, является корнем некоторого многочлена $m_i(x)$ с $i<r$, то необходимо вычислить самое большее $l-[l/q]=[\{(q-1)/q\}(l+1)]$ многочленов $m_i(x)$ для всех корней β^i, $i=1, 2, \ldots, l$ (квадратные скобки обозначают целую часть стоящей в ней дроби). Так как β является элементом $GF(q^m)$, то все многочлены $m_i(x)$ имеют степень, не превышающую m. Элемент β^0, конечно, является корнем минимального многочлена $x-1$. Таким образом, многочлен

$$\tilde{g}(x) = \prod_{\substack{i=1 \\ i\neq 0 \bmod q}}^{t-1} m_i(x) \times \begin{cases} (x-1), & m_0=0; \\ m_i(x), & m_0=1 \end{cases}$$

является многочленом степени

$$\nu = \begin{cases} \left[\frac{q-1}{q}(d-1)\right]m+1, & m_0=0; \\ \left[\frac{q-1}{q}d\right]m, & m_0=1. \end{cases} \qquad (13.33)$$

Очевидно, что порождающий многочлен $g(x)$ делит $\widetilde{g}(x)$; его степень $n-k$ не превышает, следовательно, ν и $k \geqslant n-\nu$, что и дает требуемую границу.

Рассмотрим в качестве примера класс двоичных БЧХ кодов с $m=6$. Классы сравнений и порядки e соответствующих корней приведены ниже:

0						$e=1$
1	2	4	8	16	32	63
3	6	12	24	48	33	21
5	10	20	40	17	34	63
7	14	28	56	49	35	9
9	18	36				7
11	22	44	25	50	37	63
13	26	52	41	19	38	63
15	30	60	57	51	39	21
21	42					3
23	46	29	58	53	43	63
27	54	45				7
31	62	61	59	55	47	63

(13.34)

Если $g(x)$ — минимальный многочлен, имеющий примитивный корень α, то $t=2$ [так как α^2 также является корнем $g(x)$] и получающийся (63, 57)-код имеет минимальное расстояние $d \geqslant 3$. С помощью последовательного включения все больших степеней примитивного элемента α в определение $g(x)$ получим, используя приведенные выше классы сравнений, коды со следующими параметрами:

n	63	63	63	63	63	63	63	63	63	63	63	63
k	57	51	45	39	36	30	24	18	16	10	7	1
d	3	5	7	9	11	13	15	21	23	27	31	63

Отметим, что последние восемь из этих кодов имеют размерности, бóльшие гарантированных ф-лой (13.33). Это типично, когда k малó по сравнению с n. Если корень α^0 также включается в множество корней, определяющих $g(x)$ (т. е. если $m_0=0$), то получим то же самое множество параметров, но с k, меньшим на единицу, и с d, большим на единицу.

Непримитивные элементы $GF(2^6)$ также могут быть использованы для определения БЧХ кодов. Вновь в соответствии с множеством классов сравнений в (13.34) и при выборе корня $\beta=\alpha^3$ порядка 21 получаем, что существуют БЧХ коды с параметрами

n	21	21	21	21	21
k	15	12	6	4	1
d	3	5	7	9	21.

Аналогично элементы $\beta=\alpha^7$, $\beta=\alpha^9$ и $\beta=\alpha^{21}$ определяют БЧХ коды с $n=9$, $k=3$, $d=3$ и $n=9$, $k=1$, $d=9$; с $n=7$, $k=4$, $d=3$ и $n=7$, $k=1$, $d=7$ и с $n=3$, $k=1$, $d=3$ соответственно.

Конечно, действительное построение любого из этих кодов требует задания неприводимого многочлена, соответствующего каждому из классов сравнений в (13.34). Эта задача значительно облегчается при $q=2$ в связи с тем, что имеются таблицы неприводимых многочленов.

В заключение приведем один подкласс БЧХ кодов, представляющий особый интерес, а именно, коды Рида—Соломона, которые получаются при $n=q-1$. Эти БЧХ коды имеют размерность $k\geqslant n-d+1$ [ср. с (13.33); так как d должно быть меньше, чем $q=n+1$, имеем $[\{(q-1)/q\}d]=d-1$ для всех d]. В силу того что d никогда не может превысить $n-k+1$ [см. (13.13)], эти коды являются оптимальными[1].

13.6. Перфорированные циклические коды, укороченные циклические коды и коды Хэмминга

В этом параграфе кратко рассмотрены некоторые другие кодовые конструкции, отличные от конструкций циклических кодов из предыдущего параграфа, но связанные с ними. Первая из них состоит в укорачивании циклического (n, k)-кода: требуют, чтобы i из k информационных символов были всегда нулевыми и отбрасывают эти символы из кодового слова. В силу того что циклический код является систематическим (теорема 13.12), такое множество можно получить, если потребовать, чтобы первые i символов каждого слова были нулевыми. Образующийся в результате *укороченный циклический код*, имеющий длину $n-i$ и размерность $k-i$, очевидно, остается линейным кодом, но перестает быть циклическим. В силу того что все остающиеся кодовые слова представляют собой укороченные слова первоначального циклического словаря и в силу того, что i опущенных символов были равными нулю в каждом из этих слов, минимальное расстояние между любыми двумя словами, по меньшей мере, будет таким же, как и в первоначальном словаре. В качестве примера рассмотрим двоичный циклический (7, 3)-код с расстоянием 4 (ср. с § 13.5), который может быть укорочен, если взять только те слова, начальный символ в которых равен нулю, и затем отбросить этот символ, что даст укороченный циклический (6, 2)-код, также имеющий расстояние 4: 000000, 100111, 011101, 111010.

---

[1] Можно показать, что каждый БЧХ код над полем $GF(q)$ будет подпространством (возможно укороченного) кода Рида—Соломона над некоторым более широким полем $GF(q^a)$; его кодовые слова состоят из всех тех слов кода Рида—Соломона, символы которых принадлежат лишь полю $GF(q)$. В этом смысле коды Рида—Соломона образуют более общий класс кодов. (*Прим. авт.*).

Порождающий многочлен $g(x)$ для циклических кодов является делителем многочлена x^n-1, поэтому словарь состоит из слов, соответствующих всем многочленам вида $p(x)g(x)$ по модулю x^n-1. Обобщение этого класса кодов получается, когда $g(x)$ определяется как делитель некоторого другого многочлена n-й степени $f(x)\neq x^n-1$ и кодовые слова представляются многочленами вида $p(x)g(x)$ по модулю $f(x)$. Такие коды называются *псевдоциклическими* кодами. Можно показать, однако, что каждый псевдоциклический код с минимальным весом, большим 2, является укороченным циклическим кодом и, обратно, каждый укороченный циклический код является псевдоциклическим кодом. Поэтому, кроме случая $d=2$, эти два класса кодов эквивалентны.

(Оптимальные коды с $d=2$, оказывается, существуют для всех значений n и q. Из границы Хэмминга при $d=2$ имеем $q^k\leqslant q^{n-1}$. Код, образующийся присоединением к каждой из q^{n-1} $(n-1)$-последовательностей над $GF(q)$ проверочной компоненты таким образом, чтобы сделать сумму всех n компонент равной нулю, очевидно, имеет минимальное расстояние, равное 2, и поэтому является оптимальным.)

Другой класс кодов, *перфорированные циклические коды*, получается при выбрасывании из порождающей матрицы циклического q-ичного кода максимальной длины некоторых ее столбцов. Размерность кода остается той же, но некоторые из проверочных символов опускаются. Начнем рассмотрение этих кодов, сформировав следующую теорему.

Теорема 13.13. Пусть $\mathbf{G}_k$ является матрицей размеров $k\times q^k-1$ из элементов $GF(q)$, строки которой порождают циклический код максимальной длины. Тогда каждая из q^k-1 q-ичных k-последовательностей, кроме чисто нулевой k-последовательности, появляется один и только один раз в качестве столбца $\mathbf{G}_k$.

Следствие. Каждая ненулевая q-ичная k-последовательность появляется один и только один раз в виде k последовательных символов $(\omega_i\ \omega_{i+1} \ldots \omega_{i+k-1})$ в любом слове циклического кода максимальной длины $(n=q^k-1)$ $\mathbf{w}=(\omega_0\ \omega_1 \ldots \omega_{n-1})$. [Подстрочные индексы у символов ω_i следует привести по модулю n. Например, если $i=n-2$, то, по существу, k-последовательностью будет $(\omega_{n-2}\ \omega_{n-1}\ \omega_0\ \omega_1 \ldots \omega_{k-3})$.]

Пусть теперь столбцы $\mathbf{G}_k$ разделены на $(q-1)$ *классов* так, что если столбцевой вектор $\mathbf{u}$ принадлежит первому классу, то $\alpha_2\mathbf{u}$ принадлежит второму классу; $\alpha_3\mathbf{u}$ принадлежит третьему классу и т. д., где α_i — элемент поля, над которым определяется $\mathbf{G}_k$ с $\alpha_i\neq$

$\neq\alpha_j$, $i\neq j$ и $\alpha_i\neq 0$, $\alpha_1=1$. С помощью подходящей перестановки столбцов $\mathbf{G}_k$ (которая, конечно, не меняет расстояния в результирующем словаре) получаем эквивалентную порождающую матрицу $\mathbf{G}^*_k$ в виде

$$\mathbf{G}^*_k=\alpha_1\mathbf{H}_k,\ \alpha_2\mathbf{H}_k,\ \alpha_3\mathbf{H}_k,\ \ldots,\ \alpha_{q-1}\mathbf{H}_k,$$

где $\mathbf{H}_k$ является порождающей матрицей $k\times m$ с $m=(q^k-1)/(q-1)=q^{k-1}+q^{k-2}+\ldots+1$.

Теорема 13.14. Каждое ненулевое кодовое слово из словаря, порождаемого $\mathbf{H}_k$, имеет вес $d_0=q^{k-1}$.

Следствие. Код, порождаемый матрицей, которая получается с помощью выбрасывания (перфорирования) любых r классов порождающей матрицы $\mathbf{G}_k$ циклического кода максимальной длины с размерностью k, имеет длину слова $n=(q-1-r)[(q^k-1)/(q-1)]$ и расстояние $(q-1-r)q^{k-1}$.

Мы привели примеры перфорированных циклических кодов. Для того чтобы обобщить алгоритм перфорирования, будем считать, что $\mathbf{G}_l$ является матрицей, содержащей все столбцы $\mathbf{G}_k$, имеющие нули в одних и тех же $k-l$ их компонентах. Матрица $\mathbf{G}_l$ будет порождать некоторую перестановку слов $(q^l-1,\ l)$-кода максимальной длины, но каждое слово будет повторено q^{k-l} раз. Это является следствием того, что все q^l-1 ненулевые l-последовательности представляются ненулевыми отрезками столбцов $\mathbf{G}_l$.

Разделим теперь порождающую матрицу $\mathbf{G}_k$ на $q-1$ классов, как было указано выше. Эта процедура также одновременно разделит подмножество $\mathbf{G}_l$ матрицы $\mathbf{G}_k$ на $q-1$ класс. Каждая строка каждого класса подмножества $\mathbf{G}_l$ содержит либо $(q^{l-1}-1)/(q-1)$ нулей, либо (в случае чисто нулевой строки) $(q^l-1)/(q-1)$ нулей. Следовательно, каждая из этих строк содержит самое большее q^{l-1} ненулевых элементов.

Обобщенный алгоритм перфорирования состоит в следующем. Вначале отбрасываются $q-1-t$ *классов* матрицы $\mathbf{G}_k$. Далее отбрасываются из r оставшихся t классов $\mathbf{G}_k$ все те столбцы, которые принадлежат $\mathbf{G}_l$. Кодовые слова, остающиеся к этому моменту, имеют длину $n=[t(q^k-1)/(q-1)]-r(q^l-1)/(q-1)]$, и минимальный вес равен $d=tq^{k-1}-rq^{l-1}$; размерность кода остается равной k. Затем эта процедура продолжается; выбирается другое подмножество $\mathbf{G}_{l'}$ столбцов $\mathbf{G}_k$, содержащих все столбцы, которые имеют нули во всех компонентах, кроме заданного множества из l' компонент. Если множества ненулевых компонент столбцов $\mathbf{G}_l$ и $\mathbf{G}_{l'}$ не пересекаются, то множества $\mathbf{G}_l$ и $\mathbf{G}_{l'}$ определенно не будут пересекаться. (Очевидно, что это возможно тогда и только тогда, когда $l+l'\leqslant k$.) Таким образом, можно также удалить из r' этих t классов $\mathbf{G}_k$ все столбцы, которые принадлежат $\mathbf{G}_{l'}$, образуя код с размерностью k, длиной слова $n'=[t(q^k-1)/(q-1)]-[r(q^l-1)/(q-1)]-[r'(q^{l'}-1)/(q-1)]$ и минимальным весом $d'=tq^{k-1}-rq^{l-1}-r'q^{l'-1}$. Этот процесс приводит к доказательству следующей теоремы.

Теорема 13.15. Перфорированные циклические (n, k)-коды с расстоянием d существуют для всех $n = r_0(q^k - 1)/(q-1) - \sum_{i=1}^{m} r_i(q^{l_i} - 1)/(q-1)$ и $d = r_0 q^{k-1} - \sum_{i=1}^{m} r_i q^{l_i - 1}$ при условии, что $q - 1 \geqslant r_0 \geqslant \max r_i \geqslant 0$ и $\sum_{i=1}^{m} l_i \leqslant k$. Эти коды лежат на границе (13.14), (13.15) и, следовательно, являются оптимальными.

Так как нуль-пространство подпространства само является подпространством, то оно также определяет линейный код. Рассмотрим поэтому нуль-пространство кода, натянутое на какую-либо одну порождающую матрицу из классов циклических кодов максимальной длины. Полученные коды называются кодами Хэмминга[1].

Теорема 13.16. Коды Хэмминга представляют собой линейные $(n = (q^s - 1)/(q-1),\ k = [\![(q^s - 1)/(q-1)]\!] - s)$-коды с минимальным расстоянием $d = 3$, и они существуют для всех положительных целых s. Никакой код, исправляющий одну ошибку и имеющий длину слова $n = (q^s - 1)/(q-1)$, не содержит больше слов, чем код Хэмминга с той же самой длиной слова.

13.7. Кронекеровское произведение, кронекеровская сумма и каскадные коды

Один довольно заманчивый метод построения больших кодовых словарей, исправляющих ошибки, состоит в объединении двух или большего числа меньших словарей так, чтобы сохранить желаемые их свойства в полученном большом коде. Основная трудность, с которой сталкиваются при использовании больших кодов, состоит в неизбежно связанной с ним возрастающей сложности кодирования и особенно декодирования. Если большой код получается с помощью объединения меньших кодов, то методы кодирования и декодирования часто оказываются лишь немного более сложными по сравнению с аналогичными методами, которые используются для отдельных составляющих кодов. В этом параграфе рассматриваются два метода эффективного объединения кодов.

Первая общая конструкция использует *кронекеровское произведение* порождающих матриц $\mathbf{G}_1$ и $\mathbf{G}_2$ составляющих кодов. Кронекеровское произведение $\mathbf{A} \times \mathbf{B}$ двух матриц $\mathbf{A} = \{a_{ij}\}$ и $\mathbf{B} = \{b_{ij}\}$ с элементами из одного и того же поля F определяется следующим образом:

---

[1] На самом деле, Хэмминг ограничился исследованием двоичных кодов. Здесь мы называем кодами Хэмминга все коды, которые имеют параметры, указанные в теореме 13.16. Определенные, таким образом, коды Хэмминга являются циклическими только в двоичном случае. Существуют другие циклические коды Хэмминга, хотя не для всех возможных параметров. *(Прим. авт.)*.

$$\mathbf{A}\times\mathbf{B}=\begin{bmatrix} a_{11}\mathbf{B} & a_{12}\mathbf{B} & \dots & a_{1n}\mathbf{B} \\ a_{21}\mathbf{B} & a_{22}\mathbf{B} & \dots & a_{2n}\mathbf{B} \\ \vdots & \vdots & & \vdots \\ a_{\nu 1}\mathbf{B} & a_{\nu 2}\mathbf{B} & \dots & a_{\nu n}\mathbf{B} \end{bmatrix}; \tag{13.35}$$

матрица **A** имеет размеры $\nu\times n$. Если **B** имеет размеры $\mu\times m$, то кронекеровское произведение имеет размеры $\mu\nu\times mn$. (Произведение $a\mathbf{B}$ обозначает матрицу, получаемую с помощью умножения каждого элемента **B** на элемент поля a, причем умножение, конечно, выполняется над полем F. Произведения $\mathbf{A}\times\mathbf{B}$ и $\mathbf{B}\times\mathbf{A}$ оказываются в общем случае не равными, хотя, как легко видеть, эти матрицы будут комбинаторно эквивалентными.)

Если $\mathbf{G}_1$ и $\mathbf{G}_2$ являются порождающими матрицами двух линейных кодов, то *кронекеровское произведение кодов* представляет собой код, порождаемый матрицей $\mathbf{G}_1\times\mathbf{G}_2$.

Теорема 13.17. Если $\mathbf{G}_i$ является $k_i\times n_i$ матрицей, которая порождает линейный (n_i, k_i)-код D_i, имеющий минимальное расстояние d_i, над $GF(q)$, то кронекеровское произведение кодов, порождаемое $\mathbf{G}_1\times\mathbf{G}_2$, представляет собой (n_1n_2, k_1k_2)-код, имеющий минимальное расстояние d_1d_2.

Другая полезная процедура построения связана с методом кронекеровского произведения, но приводит к кодам с меньшими размерностями и с большими минимальными расстояниями по сравнению с последним рассмотренным кодом. Из-за отсутствия лучшего названия назовем эти коды *кронекеровской суммой*[1] *кодов.* Кронекеровская сумма $\mathbf{A}\boxed{+}\mathbf{B}$ двух матриц $\mathbf{A}=\{\alpha_{ij}\}$ и $\mathbf{B}=\{\beta_{ij}\}$ определяется так:

$$\mathbf{A}\boxed{+}\mathbf{B}=\begin{bmatrix} \alpha_{11}+\mathbf{B} & \alpha_{12}+\mathbf{B} & \dots & \alpha_{1m}+\mathbf{B} \\ \vdots & \vdots & & \vdots \\ \alpha_{\mu 1}+\mathbf{B} & \alpha_{\mu 2}+\mathbf{B} & \dots & \alpha_{\mu m}+\mathbf{B} \end{bmatrix}, \tag{13.36}$$

где $\mathbf{A}$ — $\mu\times m$-матрица, а $\mathbf{B}$ — $\nu\times n$-матрица, и обе они определены над одним и тем же полем F. Сумма $a+\mathbf{B}$ означает матрицу, получаемую с помощью прибавления a к каждому элементу **B** над F.

Теорема 13.18. Пусть **A** является матрицей словаря из M слов длины m с хэмминговским расстоянием между любыми двумя словами, равным самое меньшее d_A и самое большее $m-d_A$. Аналогично пусть **B** — словарь, содержащий N слов длины n и имеющий минимальное хэмминговское расстояние d_B. Тогда матрица $\mathbf{C}=\mathbf{A}\boxed{+}\mathbf{B}$ соответствует словарю, имеющему NM слов длины mn и минимальное хэмминговское расстояние d_C такое, что $d_C\geqslant\min[md_B, nd_A]$.

Следствие. Если **A** и **B** — линейные (n_1, k)- и (n_2, k_2)-коды соответственно с минимальными расстояниями d_1 и d_2 и если максимальный вес любой строки из **A** не превышает n_1-d_1, то кронекеровская сумма кодов, представляемая **C**, также является линейным кодом с соответствующими параметрами n_1n_2, k_1+k_2 и $d_C=\min(n_1d_2,\ n_2d_1)$.

---

[1] Этот термин не следует путать с термином *«прямая сумма»*. *(Прим. авт.).*

Иногда кронекеровские произведения кодов называются также *итеративными* кодами; можно считать, что они получаются в результате итерации процедуры кодирования. Предположим, что информационные символы вначале группируются в блоки по k_2 символов и кодируются в слова длины n_2. Процесс далее может быть итерирован путем группирования этих слов в блоки по k_1 слов и добавления n_1-k_1 проверочных *слов* к каждому блоку. Если берутся i-е символы каждого из k_1 слов и осуществляется кодирование этих k_1 символов в слово длины n_1 при каждом $i=1, 2, \ldots, n_2$, то результирующий $(n_1n_2,\ k_1k_2)$-код, как легко видеть, будет кронекеровским произведением кодов. Конечно, процесс итерации может быть повторен. Это эквивалентно определению кронекеровских произведений кодов через коды, которые сами являются кронекеровскими произведениями кодов.

Эта интерпретация кронекеровских произведений кодов приводит к довольно интересному и полезному обобщению. Предположим, что вместо того, чтобы охватить второй кодовой структурой *символы* слов, образующихся после первого кодирования, мы закодируем сами *слова*, рассматривая эти слова как элементы $GF(q^{k_2})$. Это можно было бы сделать, ассоциируя с k_2 информационными символами $\alpha_1, \alpha_2, \ldots, \alpha_k$ каждого слова многочлен $p(x)=\sum_{i=1}^{k_2}\alpha_i x^{i-1}$ и выполняя арифметические операции по модулю неприводимого многочлена степени k_2. Проверочные «символы», определяемые структурой второго кода, могли бы тогда быть представлены как слова первоначального $(n_2,\ k_2)$-кода. [На практике операции кодирования, по-видимому, проходили бы в обратном порядке; информация вначале кодировалась бы над $GF(q^{k_2})$ и получающиеся «символы» затем кодировались бы над $GF(q)$.] Если второй код является линейным (n_1, k_1)-кодом (над полем из q^{k_2} элементов), то код, получающийся после объединенного кодирования, является линейным $(n_1, n_2,\ k_1, k_2)$-кодом над полем из q элементов. Более того, расстояние между любыми двумя словами этого кода, как легко показать, равно d_1d_2 — произведению расстояний двух отдельных кодов (т. е. любые два q^{k_2}-ичных кодовых слова должны отличаться, по крайней мере, в d_1 «символьных» позициях, и любые два различных «символа» должны отличаться, по меньшей мере, в d_2 местах). Такой код называется *каскадным*.

С первого взгляда кажется, что каскадные коды не дают никаких преимуществ по сравнению с кронекеровскими произведениями кодов. В обоих случаях объединение $(n_1,\ k_1)$-кода с минимальным расстоянием d_1 и $(n_2,\ k_2)$-кода с минимальным расстоянием d_2 дают $(n_1, n_2,\ k_1, k_2)$-код с минимальным расстоянием d_1d_2. Однако оба кода, являющиеся составляющими кронекеровского произведения, были определены над полем из q элементов, в то время как один из кодов, на котором основывается каскадный код, был определен над полем из q^{k_2} элементов. Если D_1 является (n_1, k_1)-кодом над $GF(q^k)$, то максимально достижимое минимальное расстояние между любыми двумя его словами будет, по меньшей мере, таким же при $k>1$, каким оно является при $k=1$. В частности, D_1 можно реализовать в виде кронекеровского произведения (n_1, k_1)-кода и (k, k)-кода, каждый из которых определен над полем $GF(q)$. Словарь, который получается при интерпретации результирующего кода с $k=k_2$ как (n_1, k_1)-кода над $GF(q^{k_2})$ и при каскадировании его с (n_2, k_2)-кодом, тождествен словарю, который получается при формировании кронекеровского произведения исходных (n_1, k_1)- и (n_2, k_2)-словарей. Следовательно, каждое кронекеровское произведение кодов можно реализовать в виде каскадного кода. Обратное утверждение неверно.

Основное преимущество при объединении малых кодов в большие коды состоит в том, что полученные коды могут быть декодированы с помощью последовательно соединенных декодеров, связанных с каждым из составляющих кодов. Каскадные коды, например, могут быть декодированы с помощью разделения, вначале принимаемой последовательности символов на блоки по n_2 символов и декодирования каждого блока в соответствии со словарем D_2. Выход этого декодера можно затем интерпретировать как последовательность n_1-символьных слов над $GF(q^{k_2})$ и декодировать в соответствии со словарем D_1. Аналогичные методы могут быть использованы для кронекеровского произведения и кронекеровской суммы кодов. Поэтому сложность декодера будет увеличиваться лишь арифметически, в то время как размерности кодов возрастают геометрически. Последовательное соединение декодеров, однако, может не исправить все ошибки, которые в действительности являются исправимыми. Некоторые комбинации, состоящие лишь из $(d_1+1)(d_2+1)/4$ ошибок, могут привести к ошибочному декодированию, когда, например, декодируются каскадные коды или кронекеровское произведение кодов, в то время как, в принципе, можно исправить вплоть до $(d_1 d_2-1)/2$ ошибок. Вместе с тем многие комбинации ошибок веса, большего, чем $(d_1+1)(d_2+1)/4$, будут исправляться последовательным соединением декодеров, и, если составляющие коды выбраны подходящим образом, суммарный результат может быть весьма удовлетворительным.

К наиболее интересным классам кодов, получаемых при использовании кронекеровских сумм, относятся классы кодов, которые получаются при последовательном кронекеровском суммировании двоичной матрицы $\mathbf{D}_1=\begin{bmatrix}0 & 0\\ 0 & 1\end{bmatrix}$ с самой собой. Результирующая матрица после i-й итерации имеет вид

$$\mathbf{D}_i=\mathbf{D}_1 \boxplus \mathbf{D}_{i-1}=\begin{bmatrix}\mathbf{D}_{i-1} & \mathbf{D}_{i-1}\\ \mathbf{D}_{i-1} & \overline{\mathbf{D}}_{i-1}\end{bmatrix},$$

$\overline{\mathbf{D}}_{i-1}$ — дополнение $\mathbf{D}_{i-1}$ (матрица, получаемая при замене каждого символа $\mathbf{D}_{i-1}$ на его дополнение). Обозначая через d_i минимальное расстояние между любыми двумя строками $\mathbf{D}_i$, согласно следствию теоремы 13.18 получаем, что так как $d_1=1=n_1/2$, то $d_i=n_i/2$ для всех i. Между прочим, эти матрицы при объединении с их дополнениями $\overline{\mathbf{D}}_i$ дают хорошо известные коды *Рида—Маллера* первого порядка. Вскоре мы встретим эти же самые коды в другом контексте.

В заключение параграфа следует упомянуть, что рассмотренные здесь методы объединения малых кодов для построения больших кодов также могут быть применены к нуль-пространствам кодов для построения новых нуль-пространств, что иногда приводит к полезным результатам.

13.8. Сверточные коды

Другим методом увеличения эффективной длины кодового слова без соответствующего увеличения сложности связанных с кодом кодера и декодера является сверточное кодирование. По-видимому, проще всего *сверточные коды* определить с помощью порождающей структуры. Порождающая матрица $\mathbf{G}$ сверточного кода имеет вид

$$\mathbf{G}=\begin{bmatrix} \mathbf{G}_0 & \mathbf{G}_1 & \mathbf{G}_2 & \ldots & \mathbf{G}_{m-1} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \ldots \\ \mathbf{0} & \mathbf{G}_0 & \mathbf{G}_1 & \ldots & \mathbf{G}_{m-2} & \mathbf{G}_{m-1} & \mathbf{0} & \mathbf{0} & \ldots \\ \mathbf{0} & \mathbf{0} & \mathbf{G}_0 & \ldots & \mathbf{G}_{m-3} & \mathbf{G}_{m-2} & \mathbf{G}_{m-1} & \mathbf{0} & \ldots \\ \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots & \vdots & \end{bmatrix}, \tag{13.37}$$

где $\mathbf{G}_l$, $l=0, 1, \ldots, m-1$ — $\mu\times\nu$-матрица с элементами из некоторого поля $GF(q)$; $G_l=\{g^{(l)}_{ij}\}$, а $\mathbf{0}$ обозначает $\mu\times\nu$-матрицу из нулей. Таким образом, если $\mathbf{x}=(x_0, x_1, \ldots)$ обозначает последовательность информационных символов [также определенную над $GF(q)$], $\mathbf{y}=(y_0, y_1, \ldots)$ обозначает последовательность символов, которые должны передаваться, то

$$\mathbf{y}=\mathbf{x}\mathbf{G}. \tag{13.38}$$

Скорость передачи информации равна μ/ν.

Вообще говоря, матрица $\mathbf{G}$ может быть полубесконечной. Поэтому сверточный код в противоположность другим кодам, рассмотренным в этой главе, не является блоковым кодом; при этом отсутствует взаимооднозначное отображение (конечных) блоков информационных символов и блоков кодовых символов. Заметим, однако, что любой символ из первых μ информационных символов влияет только на первые $m\nu$ кодовых символов. Как будет вскоре обнаружено, эта *длина кодового ограничения* $n\triangleq m\nu$ во многих отношениях аналогична длине блока (длине кодового слова) в обычных кодах, исправляющих ошибки. В последующем рассмотрении будет предполагаться, что матрица $\mathbf{G}$ систематическая, т. е.

$$g_{ij}^{(l)}=\begin{cases}1, & i=j=1,\,2,\,\ldots,\,\mu, \quad l=0;\\ 0, & i,\,j\leqslant\mu,\ i\neq j, \qquad l=0;\\ 0, & \text{при всех } i,\,j\leqslant\mu, \quad l\neq 0.\end{cases} \tag{13.39}$$

Таким образом, информационные символы будут явно появляться в кодовой последовательности $\mathbf{y}$, где $x_{i\mu+j}=y_{i\nu+j}$ при всех $i\geqslant 0$, $0\leqslant j\leqslant\mu-1$.

Так же как и в блоковых кодах, показателем относительного качества различных светочных кодов может быть минимальное хемминговское расстояние между любыми двумя кодовыми словами. Однако в силу того, что кодовые слова в сверточном коде являются (вообще говоря) бесконечно длинными, подходящее для этого случая определение расстояния менее очевидно, и оно, на самом деле, зависит от конкретно используемого алгоритма декодирования. Одним из полезных определений является минимальное расстояние d между любыми двумя различными *начальными словами* $\mathbf{y}_0=\{y_0,\,y_1,\,\ldots,\,y_{n-1}\}$, по крайней мере, одно из которых имеет некоторый ненулевой информационный символ y_i, $0\leqslant i\leqslant\mu-1$. В силу того что сверточные коды (при данном здесь определении) линейны, d соответствует минимальному весу любого начального слова, имеющего, по крайней мере, один ненулевой символ среди первых μ символов.

Смысл этого определения d состоит в следующем. Вследствие того, что длина кодового ограничения равна $n=m\nu$, первые μ информационных символов $x_i=y_i$, $0\leqslant i\leqslant\mu-1$ влияют только на начальное слово $\mathbf{y}_0$. После того как первые n символов получены на приемном конце, можно вынести решение относительно этих μ информационных символов. (Более надежное решение, однако, можно принять, если задержать момент вынесения решения.) Вообще i-е множество информационных символов $x_{i\mu+j}=y_{i\nu+j}$, $j=0,\,1,\,\ldots\,\mu-1$ влияет лишь на i-е *слово* $\mathbf{y}_i\triangleq\{y_{i\nu},\,y_{i\nu+1},\,\ldots,\,y_{n+i\nu-1}\}$. И в случае, если предшествующие $m-1$ множества информационных символов были определены правильно, их влияние на $\mathbf{y}_i$ будет известным и фактически $\mathbf{y}_i$ также будет начальным словом. Таким образом, если ранее не было совершено никаких ошибок декодирования, то d задает меру надежности, с которой может быть определено i-е множество информационных символов. (Декодер, который использует ранее декодированные символы при последующем декодировании, так как это указано здесь, называется декодером с *обратной связью*.)

Если при декодировании была сделана ошибка, то, конечно, влияние предыдущих информационных символов не будет учтено верно и последующие ошибки декодирования будут намного более вероятными. Из-за этой тенденции ошибок к распространению сверточные коды на практике часто усекаются. Это можно сделать, разделив информационные символы на блоки, например, длины

$K=(L-m+1)\mu$ и поместив после каждого блока $(m-1)\mu$ нулей. Получающийся в результате усеченный сверточный код фактически представляет собой блоковый (N, K)-код с длиной блока $N=Lv$, хотя, когда L велико, это обстоятельство не очень важно.

Так как минимальное расстояние d между начальными словами, имеющими нетождественные начальные информационные символы, представляет собой сверточный аналог для расстояния в блоковых кодах, которое рассматривалось в начальных параграфах этой главы, то интересно найти границы для этой величины, подобные тем, которые были приведены в § 13.3. Следующие две теоремы дают такие границы для расстояния d, которое в дальнейшем будем называть *начальным расстоянием*.

Теорема 13.19. Существует q-ичный сверточный $(n=m\nu, k=m\mu)$-код, имеющий минимальное расстояние, по крайней мере, равное d при любом d, удовлетворяющем неравенству

$$\sum_{j=1}^{d-1}\left[\binom{n}{j}-\binom{n-\mu}{j}\right](q-1)^j<q^{n-k}. \qquad (13.40)$$

Доказательство. Пусть $\mathbf{y}_0=\{y_0, y_1, \ldots, y_{n-1}\}$ — q-ичная n-последовательность, по крайней мере, с одной ненулевой компонентой y_i при некотором $i<\mu$ и пусть $N(\mathbf{y}_0)$ — максимальное число различных сверточных $(m\nu, m\mu)$-кодов, в которых любая такая n-последовательность является начальным словом. Далее обозначим через $N(d)$ полное число n-последовательностей вида $\mathbf{y}_0$ с весом, меньшим d. Наконец, пусть $N(m\nu, m\mu)$ обозначает число различных сверточных $(m\nu, m\mu)$-кодов. Тогда, если

$$N(\mathbf{y}_0)N(d)<N(m\nu, m\mu), \qquad (13.41)$$

то должен существовать, по крайней мере, один сверточный $(m\nu, m\mu)$-код, никакое начальное слово которого (отличное от тех, которые начинаются μ или большим числом нулем) не имеет вес, меньший, чем d, и который, следовательно, имеет начальное расстояние, по меньшей мере, равное d.

Ясно, что $N(d)$ можно получить, вычитая из полного числа q-ичных n-последовательностей веса, меньшего, чем d, число таких n-последовательностей, начинающихся μ или большим числом нулей, т. е.

$$N(d)=\sum_{j=1}^{d-1}\left[\binom{n}{j}-\binom{n-\mu}{j}\right](q-1)^j. \qquad (13.42)$$

Более того, так как имеются точно $q^{(\nu-\mu)\mu}$ различных матриц $\mathbf{G}_i$ [см. (13.37) и (13.39)] и так как m таких матриц определяют сверточный $(m\nu, m\mu$-код, то

$$N(m\nu, m\mu)=q^{m(\nu-\mu)\mu}. \qquad (13.43)$$

Остается лишь найти $N(\mathbf{y}_0)$. Для этого обозначим через η_j m-компонентный вектор, содержащий $(i\nu+j)$-е компоненты $\mathbf{y}_0$, $i=$

$=0, 1, \ldots, m-1$, т. е. $\boldsymbol{\eta}_j \triangleq \{y_j, y_{\nu+j}, \ldots, y_{(m-1)\nu+j}\}$. Пусть $\mathbf{M}_i$ обозначает треугольную $m\times m$-матрицу:

$$\mathbf{M}_i = \begin{bmatrix} x_i & 0 & 0 & \ldots & 0 \\ x_{\mu+i} & x_i & 0 & \ldots & 0 \\ x_{2\mu+i} & x_{\mu+i} & x_i & \ldots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ x_{(m-1)\mu+i} & \cdot & \cdot & & x_i \end{bmatrix},$$

где $(x_{i\mu}, x_{i\mu+1}, \ldots, x_{(i+1)\mu-1}) = (y_{i\nu}, y_{i\nu+1}, \ldots, y_{i\nu+\mu-1})$ представляет собой i-й блок информационных символов в $\mathbf{y}_0$. Пусть, наконец,

$$\gamma_{ij} = (g_{ij}^{(0)}, g_{ij}^{(1)}, \ldots, g_{ij}^{(m-1)})^T,$$

где $g^{(l)}{}_{ij}$ — (i, j)-й элемент матрицы $\mathbf{G}_l$. Тогда (13.38) означает, что

$$\eta_j = \sum_{i=0}^{\mu-1} \mathbf{M}_i \gamma_{ij}, \quad j = \mu, \mu+1, \ldots, \nu-1. \tag{13.44}$$

По крайней мере, один из x_i (пусть x_{i_0} должен быть отличен от нуля. Так как $\mathbf{M}_{i_0}$ при этом будет невырожденной, то ф-лу (13.44) можно переписать в виде

$$\gamma_{i_0 j} = \mathbf{M}_{i_0}^{-1} \left\{ \eta_j - \sum_{\substack{i=0 \\ i\neq i_0}}^{\mu-1} \mathbf{M}_i \gamma_{ij} \right\}, \quad j = \mu, \mu+1, \ldots, \nu-1. \tag{13.45}$$

Все эти уравнения должны удовлетворяться для любого сверточного кода, способного порождать начальное слово $\mathbf{y}_0$. В соответствии с этим для любого заданного $\mathbf{y}_0$ произвольные $m(\nu-\mu)$-элементов из m матриц $\mathbf{G}_l$ однозначно задаются с помощью других $m(\nu-\mu)(\mu-1)$ таких элементов и

$$N(\mathbf{y}_0) = q^{m(\nu-\mu)(\mu-1)}. \tag{13.46}$$

Подстановка ф-л (13.42), (13.43) и (13.46) в неравенство (13.45) приводит к требуемому результату.

Эта граница является сверточным аналогом границы Гилберта для блоковых кодов. Если блоковая длина отождествляется с длиной кодового ограничения, размерность блокового кода — с $m\mu$ (длиной кодового ограничения, измеренной в информационных символах), а кодовое расстояние для блокового кода —с начальным расстоянием в сверточном коде, эти две границы фактически совпадают при $\mu=1$ и $q=2$. Однако граница Гилберта была конструктивной, а ее сверточный аналог, представленный здесь, является лишь теоремой существования.

Верхние границы для расстояния, достижимого на блоковых (n, k)-кодах (§ 13.3) также, очевидно, применимы к начальному расстоянию, достижимому на сверточных кодах при замене n на длину кодового ограничения $m\nu$ и k на μ. Такие границы, конечно, не учитывают влияние возможных ненулевых информационных символов $(x_{i\mu}, x_{i\mu+1}, \ldots, x_{(i+1)\mu-1})$, $i>0$, на вес начального слова $\mathbf{y}_0$.

Типичная более плотная граница, которая принимает во внимание это влияние, приводится к следующей теореме.

Теорема 13.20. Минимальное начальное расстояние d q-ичного сверточного $(n=m\nu,\ k=m\mu)$-кода ограничено сверху неравенством

$$d \leqslant \frac{q-1}{q}\left\{n+\frac{\nu}{q^{\mu}-1}\right\}. \tag{13.47}$$

Доказательство. Очевидно, что d не может превосходить среднего веса d_{AVE} всех начальных слов $\mathbf{y}_0$, имеющих, по крайней мере, один ненулевой начальный информационный символ y_i, $i \leqslant \mu-1$. Все эти слова содержатся в подмножестве слов, порождаемых матрицей $\mathbf{M}_1$, состоящей из первых $m\mu$ строк и $m\nu$ столбцов матрицы (13.37), но не порождаемых матрицей $\mathbf{M}_2$, состоящей из последних $(m-1)\mu$ строк и $(m-1)\nu$ столбцов $\mathbf{M}_1$. Если $\mathbf{M}_1$ (и, следовательно, $\mathbf{M}_2$) не имеет чисто нулевых столбцов (такие столбцы не вносили бы вклад в расстояние получающегося кода), то она порождает словарь, содержащий в общем $N(m\nu, m\mu, q)$ ненулевых q-ичных символов, где $N(n, k, q) \triangleq nq^{k-1}(q-1)$ (см. лемму 13.4). Таким образом,

$$(q^{\mu}-1)q^{(m-1)\mu}d_{\mathrm{AVE}}=N(m\nu, m\mu, q)-N[(m-1)\nu, (m-1)\mu, q], \tag{13.48}$$

и отсюда прямо следует утверждаемое неравенство.

Методы построения хороших сверточных кодов разработаны гораздо в меньшей степени, чем методы для блоковых кодов. Большинство сверточных кодов строится с помощью некоторых процедур поиска или случайного выбора в сочетании с некоторыми эвристическими ограничениями, имеющими целью ограничить множество конкурирующих кодов теми, которые кажутся наиболее заманчивыми. Одной полезной в ряде случаев схемой построения сверточных кодов по блоковым кодам является следующая. Пусть $\mathbf{G}^{(l)}$, $l=1, 2, \ldots, m$ — набор m матриц, где $\mathbf{G}^{(l)}$ — порождающая матрица линейного блокового $(\nu, l\mu)$-кода с минимальным расстоянием d_l и где код, порождаемый $\mathbf{G}^{(l)}$, содержится в коде, порождаемом $\mathbf{G}^{(l+1)}$, при всех $l=1, 2, \ldots, m-1$. Тогда код, который получается при использовании в качестве матрицы $\mathbf{G}_i$ в (13.37) порождающей матрицы $\mathbf{G}^{(i+1)}$ (а не матрицы $\mathbf{G}^{(i)}$), будет сверточным $(m\nu, m\mu)$-кодом с минимальным начальным расстоянием, очевидно, ограниченным снизу неравенством

$$d \geqslant \sum_{l=1}^{m} d_l. \tag{13.49}$$

Заметим, что получающийся сверточный код может быть приведен к систематическому виду с помощью такого же приведения $\mathbf{G}^{(m)}$.

В качестве примера положим $\mu=1$ и будем считать, что $\mathbf{G}^{(m)}$ — кронекеровское произведение порождающей матрицы перфорированного циклического (q^{m-1}, m)-кода с расстоянием $d=(q-1)q^{m-2}$ (§ 13.6) и r-последовательности, состоящей только из ненулевых компонент. Обозначая через $\mathbf{G}_0$ rq^{m-1}-последовательность максимального веса в $\mathbf{G}^{(m)}$, получим

$$d_l = \begin{cases} rq^{m-1}, & l = 1; \\ r(q-1)q^{m-2}, & 1 < l \leqslant m. \end{cases}$$

Таким образом, описанная конструкция дает сверточный (rmq^{m-1}, m)-код с начальным расстоянием согласно ф-ле (13.49), ограниченным неравенством $d \geqslant d_0 \triangleq rq^{m-2}[(q-1)m+1]$. Но согласно (13.48) $d_0 = d_{\mathrm{AVE}}$, так что $d = d_0$, и получающийся код имеет максимально возможное начальное расстояние. Так как $d = d_{\mathrm{AVE}}$, то все начальные слова, имеющие, по крайней мере, один ненулевой начальный информационный символ, должны обладать весом d; такие коды называются *равномерными* сверточными кодами.

Другой класс сверточных кодов получается, когда матрица $\mathbf{G}^{(l)}$ порождает БЧХ код или его кодовое подпространство. Это означает, что $\mathbf{G}^{(l)}$ можно определить как подмножество порождающих матриц некоторого БЧХ (n, k)-кода (где $k \geqslant \mu l$ — размерность наименьшего БЧХ кода), содержащего все порождающие матрицы из множеств $\mathbf{G}^{(i)}$ при $i < l$. Так, если $q = 2$, $\nu = 63$ и $\mu = 1$, то $\mathbf{G}^{(1)}$ можно взять в виде порождающей матрицы двоичного БЧХ (63, 1)-кода; $\mathbf{G}^{(i)}$ — в виде подмножества порождающих матриц БЧХ (63, 7)-кода для всех $2 \leqslant i \leqslant 7$ и т. д. Поступая подобным образом, получим множество расстояний (ср. с § 13.5):

$$d_l \geqslant \begin{cases} 63, & l = 1; \\ 31, & 2 \leqslant l \leqslant 7; \\ 27, & 8 \leqslant l \leqslant 10; \\ 23, & 11 \leqslant l \leqslant 16; \\ 21, & 17 \leqslant l \leqslant 18. \end{cases}$$

Если, например, $m = 18$, то получающийся сверточный код имеет длину кодового ограничения $n = 1134$ и расстояние $d \geqslant 510$. Для сравнения верхняя граница из теоремы 13.20 ограничивает d величиной 598. Аналогично, если $\mu = 7$, получаем

$$d_l = \begin{cases} 31, & l = 1, \\ 23, & l = 2, \\ 15, & l = 3, \\ 13, & l = 4, \\ 11, & l = 5 \text{ и т. д.} \end{cases}$$

и если $m = 5$, то $n = 315$ и $d \geqslant 93$, в то время как теорема 13.20 ограничивает d сверху величиной 157.

Итак, было показано, что минимальное начальное расстояние, которое достигается на сверточных кодах, удовлетворяет границам, удивительно похожим на те, которые были получены ранее для блоковых кодов с длиной блока, равной длине кодового ограничения сверточного кода. Хотя оказалось, что найти хорошие общие конструкции сверточных кодов более трудно, чем конструкции для блоковых кодов, достаточно хорошие и в некоторых случаях оптимальные сверточные коды иногда можно построить с помощью порождающих матриц блокового кода. В силу того что с точки зрения расстояний сверточные и блоковые коды оказываются сходными, преимущества, если таковые имеются, сверточных кодов непосредственно не очевидны. К обсуждению этого вскоре возвратимся еще раз.

13.9. Кодирование и декодирование линейных кодов

Достоинства различных методов кодирования, рассмотренных выше, нельзя полностью понять, не ответив на следующие два вопроса: насколько трудно реализовать требующиеся кодер и декодер? Чему равна вероятность ошибки декодирования? Цель этого и следующего параграфов — дать, по крайней мере, частично ответы на эти вопросы.

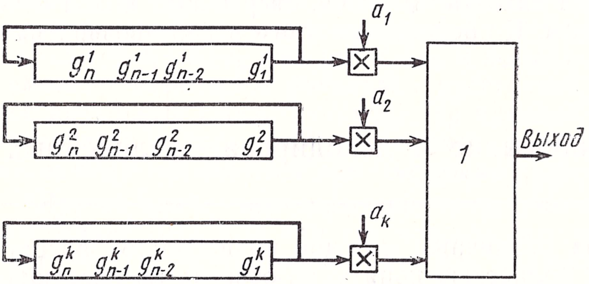
Очевидно, что эти ответы взаимосвязаны; оба они зависят от конкретного алгоритма декодирования. Как будет показано в § 13.10, вероятность ошибки P_e обычно является экспоненциально убывающей функцией длины кодового слова n. Сложность оптимального декодера может, однако, экспоненциально *возрастать* вместе с n. Это порождает сильное желание найти более просто реализуемые (возможно подоптимальные) процедуры декодирования, которые все еще сохраняют это экспоненциальное соотношение между P_e и n. Даже если получающаяся вероятность ошибки окажется больше, чем вероятность при использовании оптимального для заданного декодера n, более простой декодер вероятно мог бы быть использован при много большей длине кодовых слов, и поэтому он имел бы лучшую характеристику. Эта проблема декодирования была предметом интенсивных исследований, и сейчас известен ряд эффективных алгоритмов. Детальное описание алгоритмов выходит за рамки этой главы. Однако главные черты наиболее важных из них будут приведены здесь.

Прежде чем начать рассмотрение конкретных декодеров, уместно спросить, не возникают ли подобные же ограничения из-за свойств кодера. Вообще говоря, это не так, по крайней мере, когда рассматриваемый код линеен. Кодер линейного кода изображен на рис. 13.1. Длинные блоки на рис. 13.1 изображают циклические запоминающие устройства, а кружки обозначают умножители, выходы которых равны произведению в $GF(q)$ двух входов. Компоненты k-последовательностей $(a_1, a_2, \ldots, a_k)$, которые должны быть закодированы, используются в качестве одного из входов каждого умножителя, а k порождающих $\mathbf{g}^i = (g^i{}_1, g^i{}_2, \ldots, g^i{}_n)$, $i=$

$=1, 2, \ldots, k$, (n, k)-кода дают другие входы. Таким образом, выходом будет n-последовательность

$$\mathbf{g} = \sum_{i=1}^{k} a_i \mathbf{g}^i, \tag{13.50}$$

что и требовалось получить.



a_1
$g_n^1 \; g_{n-1}^1 \; g_{n-2}^1 \; g_1^1$
a_2
$g_n^2 \; g_{n-1}^2 \; g_{n-2}^2 \; g_1^2$
a_k
$g_n^k \; g_{n-1}^k \; g_{n-2}^k \; g_1^k$
1
Выход

Рис. 13.1. Структурная схема кодера линейного кода:
1 — сумматор в $GF(q)$

Для циклических кодов можно строить даже более экономичные кодеры. Напомним, что согласно § 13.4 циклический код ассоциирован с проверочным вектором $\mathbf{h}=(h_0, h_1, \ldots, h_k)$, таким, что $\mathbf{v}=(v_0, v_1, \ldots, v_{n-1})$ является кодовым словом тогда и только тогда, когда

$$\sum_{i=r}^{k+r} h_{i-r} v_i = \sum_{i=0}^{k} h_i v_{i+r} = 0 \tag{13.51}$$

для всех $r=0, 1, \ldots, n-k-1$. Поэтому символы v_i при $i \geqslant k$ определяются по информационным символам v_j, $j=0, 1, \ldots, k-1$ рекуррентным соотношением

$$v_{k+r} = -\frac{1}{h_k} \sum_{i=0}^{k-1} h_i v_{i+r} \stackrel{\Delta}{=} \sum_{i=0}^{k-1} \alpha_i v_{i+r}\,, \tag{13.52}$$

которое реализует декодер, изображенный на рис. 13.2. Такое устройство, называемое *регистром сдвига с обратной связью*[1]), состоит из k ячеек памяти, соединенных так, что при поступлении импульса отсчета времени (который не изображен на рисунке) содержание каждой ячейки сдвигается на одну ячейку вправо, в то время как их взвешенная [в $GF(q)$] сумма сдвигается в крайнюю левую ячейку. Если начальные данные $v_0, v_1, \ldots, v_{k-1}$, соответствующие информационным символам, помещаются в k ячеек регистра сдвига, то первые n выходных символов, выходящие из крайней правой ячейки схемы, представляют собой требуемое кодовое слово. Таким образом, весь кодер весьма компактен. По крайней мере, в случае двоичных кодов элементы кодера легко построить; умножитель по модулю два представляет собой корот-

---

[1]) См. вновь § 6.6. Там были рассмотрены (двоичные) регистры сдвига максимальной длины и были указаны свойства получающихся в результате последовательностей. Здесь рассматривается регистр сдвига с точки зрения циклического свойства кодового словаря и потому значительно многостороннее, чем в § 6.6. Заметим, что обратные связи определяются порождающим многочленом $h(x)$ нуль-пространства. (*Прим. авт.*).

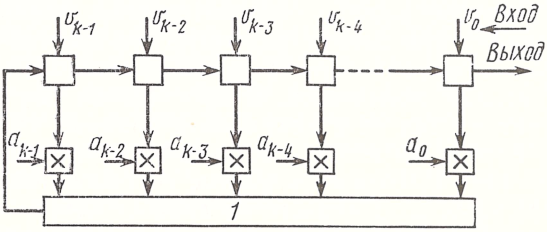


Рис. 13.2. Структурная схема кодера с регистром сдвига для циклического кода:
1 — сумматор в $GF(q)$

кое замыкание, если $\alpha_k=1$, и размыкание, если $\alpha_k=0$, а сумматор по модулю два реализуется на обычных логических элементах[1]).

Сверточные коды столь же удобны при реализации; устройство на рис. 13.3 дает пример такой реализации. Устройства, обозначенные $\mathbf{G}_i$, $i=0, 1, \ldots, m-1$, представляют собой линейные бло-

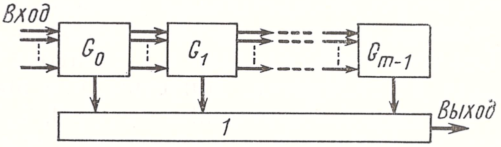


Рис. 13.3. Структурная схема кодера сверточного кода:
1 — сумматор в $GF(q)$

ковые (ν, μ)-кодеры вида, изображенного на рис. 13.1 или 13.2. Информационные символы подаются на вход первого из этих кодеров блоками по μ символов; после того как будут порождены ν кодовых символов, эти же μ символов передаются блоком в следующий кодер, а в первый кодер помещается новый блок информационных символов. Кодовые слова, которые получаются с помощью суммирования [в $GF(q)$] символов на выходах каждого из этих кодеров, как легко заметить, будут теми, которые порождаются матрицей вида (13.37).

Хотя при любом точном определении сложности кодера (или декодера) нужно принимать во внимание конкретную используемую реализацию, показатель этой сложности можно получить с помощью подсчета общего числа операций (сложений, умножений и т. д.), необходимых, чтобы закодировать (декодировать) каждый информационный символ. В соответствии с этим сложность кодера, изображенного на рис. 13.1, пропорциональна длине кодового слова n, в то время как аналогичная величина для кодера, изображенного на рис. 13.2, пропорциональна n/k. Подобно этому, сложность сверточного кодера имеет порядок самое большее $m\nu=n$. Следовательно, исключая случай, когда к кодеру при реализации предъявляются намного более жесткие требования, чем к декодеру, сложность кодера редко представляет собой ограничивающий фактор.

---

[1]) Возможно также кодировать циклические коды с помощью $(n-k)$-разрядного регистра сдвига, что приводит к очевидным преимуществам при $k>n/2$. *(Прим. авт.)*.

Возвращаясь к проблеме декодирования, отметим, что существует другое важное обстоятельство, которое нужно принять во внимание при любом рассмотрении обменных соотношений между сложностью декодера и характеристикой, а именно, вид выходного сигнала приемника. В простейшем случае выходом приемника является один из q возможных кодовых символов; в другом крайнем случае он может состоять из q уровней напряжения, соответствующих выходам фильтров, согласованных с каждым из q символов канала. С первого взгляда кажется, что твердое решение относительно каждого принятого символа должно приниматься до того, как производится декодирование. Однако, по-видимому, при декодировании будет сделано меньшее число ошибок, если декодер имеет более полную информацию относительно принятых символов. Вместе с тем использование этой информации несомненно потребует более сложного декодера. С этой точки зрения, если имеется возможность выбора вида выходного сигнала приемника, то это обстоятельство также должно быть введено в характеристику декодера наряду со сложностью.

Для того чтобы сделать эту добавочную степень свободы удобной для рассмотрения, допустим, что выходом приемника будет один из *символов приемника* r_ν, $\nu=0, 1, \ldots, N-1$. Эта модель содержит не только два упомянутых выше экстремальных случая (с $N=q$ и $N\to\infty$ соответственно), но также включает в себя многие промежуточные каналы, представляющие практический интерес. Однако здесь ограничимся, кроме двух экстремальных случаев, некоторым частным случаем общей модели приемника. В этой более ограниченной модели каждый выход приемника отождествляется с одним из возможных кодовых символов s_i, $i=0, 1, \ldots, q-1$. Кроме того, он сопоставляется с *классом верности* C_j, $j=1, 2, \ldots, J$, который дает меру уверенности, с которой это отождествление производится. Таким образом, символы приемника r_ν принимают вид $s^{(j)}{}_i$, где подстрочный индекс обозначает кодовый символ, с которым отождествляется r_ν, а надстрочный индекс — его класс верности.

Пусть $\Pr\{s^{(j)}{}_i|s_\nu\}$ обозначает вероятность получения $s^{(j)}{}_i$, если послан символ s_ν. Канал (который, конечно, включает в себя приемник), связанный с этой моделью, будет предполагаться симметричным в том смысле, что вероятности $\Pr\{s_i^{(j)}\mid s_\nu\}\overset{\Delta}{=}\begin{cases}p_{cj}, & \nu=i;\\ p_{ej}, & \nu\neq i\end{cases}$ не зависят ни от i, ни от ν. Для удобства классы верности упорядочены так, чтобы $\Pr\{s_i|s^{(j)}{}_i\}$ (вероятность того, что был передан s_i, когда принимается $s^{(j)}{}_i$) была убывающей функцией j. В общем, будет предполагаться также, что p_{cj} больше или равны p_{ej} при всех j.

За исключением случая $q=2$, приемники с классами верности обычно разрушают существенную информацию относительно принятых символов даже тогда, когда число классов J стремится к бесконечности. Тем не менее эта модель описывает многие практически интересные ситуации. Если, например, $J=2$ и выход приемника отождествляется либо с одним из q кодовых символов, либо с $(q+1)$-м символом, который с равной вероятностью может быть любым из них $(p_{c2}=p_{e2})$, то получающийся канал называется каналом со *стираниями*. Обычно эта модель возникает, когда символы приемника получаются с помощью квантования наибольшего выхода из q-выходов согласованных фильтров, опять-таки при предположении, что вероятность ошибочной замены одного символа на другой не зависит от обоих рассматриваемых символов.

После этих предварительных замечаний опишем некоторые из наиболее важных алгоритмов декодирования.

Декодирование максимального правдоподобия. Обозначим через $\mathbf{w}_\nu$ ν-е n-символьное слово в кодовом словаре, а через $\mathbf{v}$ — n-последовательность символов приемника, соответствующих некоторому принятому слову. Тогда в предположении, что все слова кода передаются с равными вероятностями, оптимальный декодер (в смысле минимума вероятности ошибки в слове) декодирует вектор $\mathbf{v}$ в виде $\mathbf{w}_l$, где

$$\max_{\nu} \Pr\{\mathbf{v} \mid \mathbf{w}_\nu\} = \Pr\{\mathbf{v} \mid \mathbf{w}_l\}, \tag{13.53}$$

т. е. оптимальный декодер является *декодером максимального правдоподобия*. Если статистики в канале не зависят от символа, то

$$\Pr\{\mathbf{v} \mid \mathbf{w}_\nu\} = \prod_{\mu=1}^{n} \Pr\{\eta_\mu \mid \omega_\mu(\mathbf{v})\}, \tag{13.54}$$

где $\omega_\mu(\mathbf{v})$ и $\boldsymbol{\eta}_\mu$ — соответственно μ-е символы в $\mathbf{w}_\nu$ и $\mathbf{v}$. В общем случае для любого μ каждый из кодовых символов s_i будет использоваться как μ-й символ некоторого кодового слова. Следовательно, декодер максимального правдоподобия должен тем или иным образом найти nq вероятностей $\Pr\{\boldsymbol{\eta}_\mu | \omega_\mu(\mathbf{v})\}$ и сформировать q^k различных произведений этих вероятностей. Сложность декодера (на информационный символ), следовательно, пропорциональна $(n/k)q^k$ и при фиксированной скорости k/n фактически является экспоненциально возрастающей функцией длины блока n.

Трудность вычисления вероятности $\Pr\{\boldsymbol{\eta}_\mu | \omega_\mu(\mathbf{v})\}$, очевидно, зависит от статистик канала. Как было показано в гл. 4, они, например, относительно легко находятся, когда канал является фазовокогерентным гауссовским каналом, и несколько труднее, когда канал фазовонекогерентный. В любом случае часто удобно ограничить алфавит приемника. Значительное упрощение декодера достигается, когда приемник является приемником с классами верности того типа, который был описан выше. При этом (13.54) записывается в виде

$$\Pr\{\mathbf{v} \mid \mathbf{w}_\nu\} = \prod_{j=1}^{J} p_{ej}^{n_{ej}^{\nu}} p_{cj}^{n_{cj}^{\nu}} = \exp \sum_{j=1}^{J} \left\{ n_j \log p_{cj} - n_{ej}^{\nu} \log\left(\frac{p_{cj}}{p_{ej}}\right)\right\}, \tag{13.55}$$

где $n^{\nu}{}_{cj}$ — число случаев, когда символ вида $s^{(j)}{}_i$ в $\mathbf{v}$ соответствует символу $\mathbf{s}_i$ в $\mathbf{w}_\nu$; $n^{\nu}{}_{cj}$ — число случаев, когда $s^{(j)}{}_i$ в $\mathbf{v}$ соответствует s_μ в $\mathbf{w}_\nu$ для некоторого $\mu \neq i$, а $n_j = n^{\nu}{}_{ej} + n^{\nu}{}_{ij}$ не зависит от ν. Декодер максимального правдоподобия декодирует при этом $\mathbf{v}$ в виде $\mathbf{w}_l$ в том случае, если

$$d_\nu \triangleq \sum_{j=1}^{J} n_{ej}^{\nu} \frac{\log_e (p_{cj}/p_{ej})}{\log_e (p_{c1}/p_{e1})} \triangleq \sum_{j=1}^{J} \alpha_j n_{ej}^{\nu} \tag{13.56}$$

принимает максимальное значение при $\nu = l$. (Если это имеет место для более чем одного значения l, то может быть выбрано любое из таких кодовых слов $\mathbf{w}_l$.)

Если $J=1$, то d_ν представляет собой просто хэмминговское расстояние между выходом канала $\mathbf{v}$ и ν-м кодовым словом $\mathbf{w}_\nu$, и декодер максимального правдоподобия отыскивает кодовое слово, ближайшее в смысле Хэмминга к принятой n-последовательности. Это обстоятельство делает возможным использование алгебраической структуры кода для снижения в какой-то мере сложности декодера максимального правдоподобия. Так как $\mathbf{v}$ теперь является q-ичной n-последовательностью, то оно принадлежит некоторому смежному классу линейного кодового словаря D. Декодер максимального правдоподобия поэтому должен лишь найти смежный класс, к которому принадлежит $\mathbf{v}$, и вычесть из $\mathbf{v}$ вектор, который называется *лидером смежного класса* (и который определяется здесь, как любая из n-последовательностей минимального веса в смежном классе). Действительно, если $\mathbf{v}—\mathbf{c}$ принадлежит D, то $\mathbf{v}$ и $\mathbf{c}$ должны лежать в одном и том же смежном классе; так как $\mathbf{c}$ является элементом с минимальным весом в смежном классе, содержащем $\mathbf{v}$, то в D не может быть слова, более близкого к $\mathbf{v}$, чем $\mathbf{v}—\mathbf{c}$.

Относительно простой метод определения смежного класса, в котором находится принятое слово, описывается следующей теоремой. Пусть $\mathbf{H}$ — порождающая матрица нуль-пространства (n, k) кодового словаря D. Тогда определим *синдром* $\mathbf{s}$ вектора $\mathbf{v}$, как $\mathbf{s} = \mathbf{v}\mathbf{H}^T$. Вектор $\mathbf{s}$ имеет над $GF(q)$ размерность $n-k$.

Теорема 13.21. Векторы $\mathbf{v}_1$ и $\mathbf{v}_2$ принадлежат одному и тому же смежному классу линейного кодового словаря D тогда и только тогда, когда равны их синдромы $\mathbf{s}_1$ и $\mathbf{s}_2$.

Таким образом, декодирование может быть выполнено, если хранить в памяти q^{n-k} лидеров смежных классов, отождествив их со связанными с ними синдромами. Когда принимается $\mathbf{v}$, определяется синдром $\mathbf{s} = \mathbf{v}\mathbf{H}^T$. Соответствующий лидер смежного класса затем вычитается из первоначального вектора **v**. Во многих случаях этот метод реализуется намного проще, чем более прямая процедура отыскания расстояния между каждым словом словаря и принятым словом. Это, в частности, справедливо в случае циклических кодов, так как произведение $\mathbf{vH}^T$ находится с помощью умножения соответствующего многочлена $v(x)$ на порождающий многочлен $h(x)$ нуль-пространства и приведения результата по модулю x^n-1. Эту операцию нетрудно реализовать.

Для эффективного использования структуры кода не обязательно, чтобы алфавиты кода и приемника совпадали. Декодеры максимального правдоподобия были разработаны для некоторых кодов, построенных с помощью кронекеровских сумм, и они требуют лишь примерно $n \log_e n$ операций даже в когерентном гауссовском канале. (Скорость передачи для этих кодов стремится к нулю асимптотически по n, так что это утверждение нужно принимать с соответствующей оговоркой.)

Алгебраическое декодирование. Если алфавиты приемника и кода совпадают, то принятое слово **v** имеет вид $\mathbf{v}=\mathbf{w}+\mathbf{e}$, где **w** — кодовое слово, а $\mathbf{e}=(e_1, e_2, \ldots, e_n)$ — вектор ошибки с компонентами из кодового поля $GF(q)$. Если рассматриваемый код линеен и если **H** — порождающая матрица его нуль-пространства, то, считая, что **v**, **w** и **e** являются векторами-строками, имеем

$$\mathbf{vH}^T=(\mathbf{w}+\mathbf{e})\,\mathbf{H}^T=\mathbf{eH}^T. \tag{13.57}$$

Таким образом, структура кода определяет систему $n-k$ уравнений с n неизвестными e_i. Это система уравнений не будет иметь однозначного решения; каждая такая система в действительности имеет q^k решений, так как, если **e** — решение, то решением также будет $\mathbf{e}+\mathbf{w}$ при любом кодовом слове **w**. Тем не менее свойства расстояния в коде гарантируют самое большее одно решение с $[(d-1)/2]$ или меньшим числом ненулевых компонент. В соответствии с этим, по крайней мере, когда число ошибок при передаче не превышает $[(d-1)/2]$, уравнение (13.57) может быть решено однозначно относительно **e** и может быть определено правильное кодовое слово $\mathbf{w}=\mathbf{v}-\mathbf{e}$.

Термин *алгебраическое декодирование* относится к классу алгоритмов декодирования, в которых с помощью регулярного метода отыскивается решение **e** системы ур-ний (13.57) с минимальным весом. Чаще всего эти алгоритмы заведомо работают только тогда, когда существует решение **e** с весом $[(d-1)/2]$ или меньшим. В частности, высокоэффективные алгебраические процедуры декодирования были развиты для циклических БЧХ кодов, рассмотренных в § 13.6. Сложность БЧХ декодеров может быть доведена до величины порядка $n \log_e n$, что означает значительное улучшение по сравнению с экспоненциальной зависимостью от длины кодового слова, типичной для декодеров максимального правдоподобия. Требуемые декодеры становятся, однако, значительно более сложными при попытке исправлять более чем $[(d-1)/2]$ ошибок.

Все операции при алгебраическом декодировании выполняются в поле $GF(q)$, над которым определен код. Это означает, что алфавиты приемника и кода должны совпадать. Однако с помощью небольшого увеличения сложности алгебраические декодеры могут быть приспособлены также для обработки стираний. Арифметические операции в этом случае продолжают выполняться над $GF(q)$, но декодер также опознает возможные «пустые символы», которые он считает абсолютно неизвестными.

Легко видеть, что любая комбинация e ошибок и t стираний может быть исправлена, если $2e+t<d$, где d — минимальное хэмминговское расстояние между любыми двумя кодовыми словами. Так, если два n-символьных слова отличаются, по крайней мере, в d символах, то подмножество любых $n-t$ их символов должно отличаться, по крайней мере, в $d-t$ позициях. Таким образом, должно произойти самое малое $[(d-t+1)/2]$ ошибок для того, чтобы кодовое слово, в котором произошло t стираний, трансформировалось в вектор, который, по крайней мере, также близок ко второму кодовому слову, как и к первоначальному.

Удивительно, что незначительная модификация в сочетании с обычным приемником с классами верности позволяет эффективно применять алгебраический декодер в случае, когда имеются как ошибки, так и стирания.

В основе этого утверждения лежит следующая лемма.

Лемма 13.5. Пусть k_1 и k_2 и множества $\{m_j\}$ и $\{n_j\}$, $j=1, 2, \ldots, J$ представляют собой произвольные постоянные, и пусть $\{\alpha_j\}$ — множества из J коэффициентов, таких, что $1 \geqslant \alpha_1 \geqslant \alpha_2 \geqslant \ldots \geqslant \alpha_J \geqslant 0$. Тогда неравенство

$$\sum_{j=1}^{J} \alpha_j m_j < k_1 - k_2 \sum_{j=1}^{J} (1-\alpha_j) n_j \tag{13.58}$$

влечет за собой

$$\sum_{j=1}^{l} m_j < k_1 - k_2 \sum_{j=l+1}^{J} n_j \tag{13.59}$$

для некоторого $0 \leqslant l \leqslant J$ [1]).

Теорема 13.22. Пусть D — линейный (n, k) кодовый словарь, имеющий минимальный хэмминговский вес d. Пусть $\mathbf{v}$ — выход приемника с классами верности, соответствующий некоторому переданному кодовому слову $\mathbf{w}_\mu$, и пусть α_j — вес, приписанный j-му классу верности C_j, где $1 \geqslant \alpha_1 \geqslant \alpha_2 \geqslant \ldots \geqslant \alpha_j \geqslant 0$. Далее пусть n^{ν}_{ej} — число случаев, когда j-й символ класса верности в принятой

---

[1]) Суммы вида $\sum\limits_{j=\nu}^{\nu-1} x_j$ считаются равными нулю. (*Прим. авт.*).

n-последовательности $\mathbf{v}$ отличается от соответствующего символа в кодовом слове $\mathbf{w}_\nu$, и пусть n_j — полное число символов в $\mathbf{v}$ из этого класса верности. Тогда, если существует такое $\mathbf{w}_\nu$, что

$$\sum_{j=1}^{J} \alpha_j n_{ej}^{\nu} < \frac{d - \sum\limits_{j=1}^{J} (1-\alpha_j)\, n_j}{2}, \qquad (13.60)$$

то справедливы следующие утверждения: 1) $\mathbf{w}_\nu$ единственно; 2) $\mathbf{w}_\nu$ входит в множество слов, получаемых с помощью алгебраического декодирования $\mathbf{v}$ с символами из $J-1$ классов наименьшей верности, рассматриваемыми в качестве стираний, и остальными, которым приписывается вес единица для всех l из интервала $[1, J]$.

Напомним, что декодер максимального правдоподобия, связанный с приемником с классами верности, декодирует принятую n-последовательность $\mathbf{v}$ как $\mathbf{w}_\nu$ только тогда, когда *обобщенное минимальное расстояние* $d_\mu = \sum\limits_{j=1}^{J} \alpha_j n_{ej}^{\mu}$ достигает минимального значения при $\mu=\nu$. Смысл теоремы 13.22 состоит в том, что если d_ν меньше, чем $\{[d - \sum\limits_{j=1}^{J} (1-\alpha_j) n_j]/2\}$ для некоторого ν, то алгебраический декодер способен найти слово $\mathbf{w}_\nu$, рассматривая все принятые символы в $J-l$ классах наименьшей верности как стирания, а остающиеся символы как максимально надежные. После каждого такого декодирования декодированное слово, если таковое окажется, может быть проверено с тем, чтобы узнать, удовлетворяет ли оно неравенству (13.60). Если удовлетворяет, то декодирование оканчивается; если нет, критерий стирания изменяется, и делается новая попытка. Предполагается, что такой декодер может отыскать слово, удовлетворяющее неравенству (13.60) при каждом используемом значении l. Тем не менее лишь одно самое большее из этих слов будет удовлетворять неравенству (13.60). Более того, число попыток декодирования самое большее равно $[(d+1)/2]$. Дело в том, что при наличии $t+1$ стираний декодер может исправить столько же ошибок, сколько и при наличии t стираний, если t и d либо оба четны, либо оба нечетны. Таким образом, если $t+1$ стираний возникают вследствие стирания символов в $(J-l)$ классах наименьшей верности, а t стираний — из-за стирания в $(J-l-1)$ классах наименьшей верности, то вторую попытку можно не делать, она не сможет дать какое-либо слово, уже не найденное при предыдущей попытке. Далее, если t превышает $d-1$, то не нужны обе попытки, так как в этом случае условие (13.60), по-видимому, не может быть удовлетворено.

Во всем этом рассмотрении единственными условиями, налагаемыми на коэффициенты α_j, были требования, чтобы они лежали в интервале $0 \leqslant \alpha_j \leqslant 1$ и чтобы они представляли собой невозрастающие функции j. При этих условиях для определения обобщенного расстояния d_ν можно использовать любое множество коэффициентов. Как было показано, оптимальный выбор α_j при декодировании максимального правдоподобия задается соотношением (13.56). Однако эти коэффициенты не обязательно являются оптимальными при декодировании по максимуму обобщенного расстояния. Этот вопрос будет изучаться в § 13.10.

Вероятностное декодирование. При использовании методов алгебраического декодирования пытаются уменьшить сложность декодирования по сравнению со сложностью декодирования максимального правдоподобия с помощью использования алгебраической структуры кода. При использовании методов вероятностного декодирования стараются достичь ту же цель с помощью замены одного сложного решения (относительно того, какое кодовое слово было получено) рядом более простых. По существу, для этого используются деление принятого слова на отрезки и определение, возможно временное, подмножества кодовых слов, наиболее правдоподобно согласующихся с каждым последовательным отрезком. Если эти подмножества взаимно состоятельны (т. е. если, по крайней мере, одно кодовое слово принадлежит каждому подмножеству), то декодер продолжает декодирование до тех пор, пока он, наконец, не придет к единственному слову. Если в какой-либо момент времени эта процедура столкнется с трудностью (если ни одно из кодовых слов, которые все еще остаются среди конкурирующих, не обещает в перспективе оказаться верным), то возможно возвращение назад для пересмотра ранее принятых решений и выбора для дальнейшего рассмотрения другого подмножества кодовых слов.

Таким образом, вероятностный декодер рассматривает лишь малую долю принятых кодовых слов в любой момент времени, и отсюда следует, что связанная с ним сложность реализации уменьшается. Число операций, однако, и, следовательно, время, необходимое для вынесения решения, часто теперь является случайной величиной (зависящей от конкретного используемого алгоритма) и может в ряде случаев превышать время до момента, когда возникает необходимость декодирования нового слова.

Среди наиболее эффективных вероятностных схем декодирования следует назвать *алгоритмы последовательного декодирования,* предназначенные для использования со сверточными кодами. Причина, по которой вероятностный подход особенно эффективен для сверточных кодов, очевидна. Первые ν кодовых символов сверточного кодового слова полностью определяются первыми μ информационными символами (см. § 13.8). Таким образом, предварительное решение относительно этих μ информационных символов может быть сделано после того, как будут приняты лишь ν кодовых символов. Это первоначальное решение фактически снижает число конкурирующих кодовых слов в $q^{-\mu}$ раз, так же как и каждое последующее решение, выносимое после получения каждого последующего блока из ν символов. Если какой-либо из этих блоков по ν символов содержит слишком много ошибок, то будет принято неправильное решение, и правильное кодовое слово окажется среди тех, которые временно будут устранены из рассмотрения. Однако при дальнейшем декодировании, вероятно, будет сделано предположение, что произошла ошибка на ранней стадии (никакое из конкурирующих кодовых слов не будет удовлетворительно согласовываться с последовательными блоками принимаемых символов), и это ошибочное решение с большой вероятностью будет пересмотрено в некоторый более поздний момент.

Вероятностный подход может также быть эффективно использован для некоторых классов линейных блоковых кодов. В этом случае правильность решения относительно каждого последовательного символа оценивается на основе всех тех принятых символов, которые вместе с ним входят в проверочные соотношения, определяемые структурой кода. Если бы каждая оценка была верной, то слово было бы декодировано сразу после n таких операций. (В действительности было бы достаточно k операций, так как должны быть определены лишь информационные биты.) Однако в общем случае некоторые из этих оценок будут неверными и потребуется несколько итераций, причем каждая оценка предыдущей итерации будет пересматриваться на основе других оценок, полученных во время этой итерации. Если все оценки являются состоятельными (т. е. если текущие оценки удовлетворяют всем проверочным соотношениям), то принимаемая n-последовательность декодируется. Фактически число конкурирующих кодовых слов временно снижается на каждом шаге процедуры декодирования с помощью оценивания одного из принимаемых символов. Если оценка верна, то принимаемое слово должно принадлежать подмножеству кодовых слов, имеющих этот символ на этой позиции; если оценка ошибочна, то сохраняется надежда, что она будет исправлена на одной из последующих итераций.

Более подробные сведения относительно вероятностных алгоритмов декодирования можно найти в литературе. Здесь достаточно будет отметить, что такие методы могут быть весьма эффективными во многих приложениях. В то время как число операций, необходимых для алгебраического декодирования слова, примерно постоянно и не зависит от числа ошибок, которые оно содержит, вероятностные алгоритмы декодирования обычно требуют случайного числа операций, которое сильно зависит от возникших в канале помех. Тем не менее при вероятностном алгоритме среднее число операций при декодировании может оказаться меньшим для заданной длины слова или длины кодового ограничения n по сравнению с алгебраическим. Фактически среднее число операций на информационный символ, необходимых для последовательного декодирования сверточного кода, оказывается функцией лишь параметров μ и ν (ср. с § 13.9) и статистик канала; оно, по существу, не зависит от длины кодового ограничения n.

Пороговое декодирование. Прежде чем окончить рассмотрение методов декодирования, упомянем еще один подход к задаче декодирования, который не является полностью ни вероятностным, ни алгебраическим, но имеет ряд общих с ними черт. Этот метод декодирования, который называется *пороговым декодированием,* особенно эффективен для некоторых классов кодов как блоковых, так и сверточных. Для того чтобы использовать этот алгоритм, необходимо отобрать из множества проверочных уравнений, порождаемых проверочной матрицей **H** подмножество E_i уравнений, *ортогональных* для i-го символа w_i кодового слова. Это означает, что каждое уравнение из множества E_i должно содержать w_i в проверочном соотношении наряду с другими символами w_j, $j \neq i$, но так, чтобы ни один символ, кроме w_i, не входил более чем в одно из этих уравнений.

Предположим, что принимается последовательность $(w_1+e_1, w_2+e_2, \ldots, w_n+e_n)$, где w_j означает j-й символ некоторого кодового слова, а e_j — символ ошибки. Каждое уравнение из ортогонального множества E_i дает тогда независимую оценку $\hat{w}_i$ величины w_i, т. е. $\hat{w}_i(\nu)$ — кодовый символ, который удовлетворяет ν-му уравнению из множества E_i. Если E_i содержит d'_i-1 уравнений, то в силу того, что i-й принятый символ w_i+e_i также дает независимую оценку для w_i, декодер может легко определить d'_i таких оценок. Если не более $[(d'_i+1)/2]$ символов ошибок e_j, входящих в эти уравнения, отличны от нуля, то более половины получающихся оценок будут определены верно, и простое решение по большинству этих оценок будет давать правильное значение w_i. В соответствии с этим, если каждое множество E_i, $i=1, 2, \ldots, n$ содержит, по меньшей мере, $d'-1$ уравнений и если принятое кодовое слово содержит $[(d'-1)/2]$ или меньше ошибок, то слово будет правильно декодировано декодером, работающим по этому принципу. На этом и основан пороговый алгоритм декодирования.

Если множества E_i могут быть найдены для каждого i и они содержат, по крайней мере, $d-1$ уравнений, где d — минимальное хэмминговское расстояние между любыми двумя словами кодового словаря, то говорят, что код *полностью ортогонализуемый.* Если код полностью ортогонализуемый (а некоторые коды являются таковыми), то пороговый декодер может исправлять любую комбинацию ошибок, которую могли бы исправить большинство алгебраических декодеров. Более того, пороговым декодером могут быть исправлены многие комбинации ошибок, содержащие более чем $e=[(d-1)/2]$ ошибок. Хотя алгебраический декодер также иногда можно видоизменить так, чтобы он исправлял более чем e ошибок, это можно сделать лишь за счет значительного увеличения сложности.

В общем случае не все уравнения из множества E_i содержат одно и то же число принятых символов. Надежность оценки $\hat{w}_i(\nu)$, очевидно, будет зависеть до некоторой степени от числа принятых символов, которые используются при отыскании этой оценки. Вследствие этого характеристика порогового декодера иногда может быть улучшена с помощью взвешивания каждой оценки $\hat{\omega}_i(\nu)$ в соответствии с вероятностью того, что она верна, а не так, как это делается при описанном выше построении решения по большинству этих оценок.

13.10. Вероятности ошибочного декодирования

Вероятность ошибочного декодирования зависит не только от статистик канала и конкретно выбранного кода, но, очевидно, также от алгоритма декодирования. Даже обладая этой информацией, часто трудно определить точные выражения для вероятности ошибки. Например, вероятность ошибки, связанная с декодированием максимального правдоподобия линейных кодов, может быть найдена только, если известна вся весовая структура кода. Вероятность спутать одно слово с другим является функцией расстояния между двумя рассматриваемыми кодовыми словами независимо от минимального расстояния кода.

Ситуация усложняется еще больше, когда число символов приемника велико по сравнению с числом кодовых символов. Однако обычно намного легче получить полезные границы для вероятности ошибки. Например, границы гл. 4 прямо применимы здесь, если канал является фазовокогерентным гауссовским каналом. Декодер максимального правдоподобия для такого канала разыскивает максимум по ν функции вида $\log_e \Pr\{\mathbf{v} | \mathbf{w}_\nu\} = \sum_\mu \log_e \Pr\{\boldsymbol{\eta}_\mu | \omega_\mu(\nu)\}$ (см. § 13.9). Так как $\log_e \Pr\{\boldsymbol{\eta}_\mu | \omega_\mu(\nu)\}$ является линейной функцией корреляции между принятым сигналом и сигналом, представляющим $\omega_\mu(\nu)$, то решение относительно принятого слова остается тем же самым, независимо от того, основывается ли процедура декодирования на посимвольном решении (в силу того, что не теряется никакая информация) или принятое *слово* коррелируется с каждым из возможных кодовых слов. Единственное влияние структуры кода на принятый сигнал состоит в потенциальном снижении сложности приемника, которое она допускает.

В этом параграфе будет получена верхняя граница для вероятности ошибки в слове, когда используется декодирование по обобщенному минимальному расстоянию, определенное в § 13.9. Рассмотрим этот частный случай в силу нескольких причин. Во-первых, в силу общности этого правила декодирования сама граница является весьма гибкой. Во-вторых, она показывает в удобной форме связь между вероятностью ошибки и имеющими к ней отношение параметрами кода. И, наконец, она также пригодна в качестве границы для вероятностей ошибок, связанных с многими другими представляющими интерес правилами декодирования, включая не только декодирование максимального правдоподобия, но и все те алгоритмы, в которых выход приемника содержит (а декодер использует) больше информации, чем приемник с классами верности сам по себе.

Граница определяется следующей теоремой.

Теорема 13.23. Если q-ичное n-символьное слово из словаря D с минимальным расстоянием d передается по каналу с шумом и декодируется по обобщенному минимальному расстоянию, то вероятность P_e ошибочного декодирования ограничена неравенством

$$P_e \leqslant \min_{s\geqslant 0} \exp\left\{-n\left[s\frac{d}{n} - \mu(s)\right]\right\}, \tag{13.61}$$

где $\mu(s) = \log_e \sum_{j=1}^{J} \left\{p_{cj}\, e^{s(1-\alpha_j)} + (q-1)p_{ej}\, e^{s(1+\alpha_j)}\right\}$; p_{ej}, p_{cj} и α_j определены ранее (см. с. 392 и теорему 13.22).

Доказательство. Ошибочное декодирование совершается только тогда, когда неравенство (13.60) нарушается при условии, что $\mathbf{w}_\nu$ — в действительности переданное слово. Таким образом,

$$P_e = \Pr\left\{\sum_j \alpha_j n_{ej}^{\nu} \geqslant \frac{d - \sum\limits_j (1-\alpha_j) n_j}{2} \mid \nu\right\} =$$

$$= \Pr\left\{\sum_j \left[(1+\alpha_j) n_{ej}^{\nu} + (1-\alpha_j) n_{cj}^{\nu}\right] \geqslant d \mid \nu\right\}. \tag{13.62}$$

Пусть y_i — дискретная случайная величина с распределением $p(y_i) = \sum\limits_j \{(q-1)p_{ej}\delta[y_i-(1+\alpha_j)] + p_{cj}\delta[y_i-(1-\alpha_j)]\}$. Тогда y_i принимает значение $(1+\alpha_j)$ с вероятностью $(q-1)p_{ej}$ (это вероятность того, что символ приемника находится в классе C_j и отождествляется с *каким-либо* q-ичным символом, отличным от фактически переданного) и значение $(1-\alpha_j)$ с вероятностью p_{cj} (это вероятность того, что символ приемника находится в классе C_j и отождествляется с переданным символом). В соответствии с этим

$$\Pr\left\{\sum_j \left[(1+\alpha_j) n_{ej}^{\nu} + (1-\alpha_j) n_{cj}^{\nu}\right] \geqslant \mid \nu\right\} = \Pr\{z \geqslant d\}, \tag{13.63}$$

где $z = \sum\limits_{i=1}^{J} y_i$. Пусть $\{z_j\}$ обозначает множество значений, принимаемых случайной величиной z. Тогда для любого $s \geqslant 0$ имеем

$$\Pr\{z \geqslant d\} = \sum_{\substack{\text{по всем} \\ z_j \geqslant d}} p(z_j) \leqslant e^{-sd} \sum_{\substack{\text{по всем} \\ z_j}} e^{sz_j} p(z_j), \tag{13.64}$$

где неравенство следует из того, что $e^{-s(d-z)}$ является неотрицательным для всех z и, по меньшей мере, равно единице для всех $z \geqslant d$. Продолжая, получаем

$$P_e = \Pr\{z \geqslant d\} \leqslant e^{-sd} E(e^{sz}) = e^{-sd} E\left(\prod_{i=1}^{n} e^{sy_i}\right) = e^{-sd} \prod_{i=1}^{n} E(e^{sy_i}). \tag{13.65}$$

Последнее равенство является следствием предполагаемой независимости последовательных ошибок в символах, а значит, случайных величин y_i. Так как

$$E\left(e^{sy_i}\right)=\sum_{j=1}^{J}\left[(q-1)\,p_{ej}\,e^{s(1+\alpha_j)}+p_{cj}\,e^{s(1-\alpha_j)}\right], \tag{13.66}$$

то теорема доказана.

Наиболее точная верхняя граница для P_e получается, когда показатель экспоненты в квадратных скобках в ф-ле (13.61) максимизируется по s, т. е. когда $\mu'(s)=d/n$. Как легко проверить, $\mu''(s)$ положительна при всех s (за исключением тривиального случая, в котором все α_j равны и $\sum\limits_j p_{cj}=0$ или 1). Таким образом, поскольку $\mu'(\infty)=\max\limits_j(1+\alpha_j)>d/n$, функция $s(d/n)-\mu(s)$ имеет единственный максимум для некоторого s, $0<s<\infty$ только тогда, когда $\mu'(0)<d/n$. Но, если $\mu'(0)<d/n$, то верхняя граница (13.61) является экспоненциально убывающей функцией длины слова n.

Параметры α_j также можно выбрать так, чтобы минимизировать границу для P_e. Дифференцируя показатель экспоненты границы (13.61) по α_j и вспоминая, что α_j должны лежать между 0 и 1, найдем, что наименьшая граница получится, если

$$\alpha_j=\begin{cases}1 & \text{при } \log_e\dfrac{p_{cj}}{(q-1)\,p_{ej}}\geqslant 2s;\\[2ex] 0 & \text{при } \log_e\dfrac{p_{cj}}{(q-1)\,p_{ej}}\leqslant 0;\\[2ex] \dfrac{1}{2s}\log_e\dfrac{p_{cj}}{(q-1)\,p_{ej}} & \text{в остальных случаях.}\end{cases} \tag{13.67}$$

Наилучшая граница сверху для вероятности ошибки (13.61) получится, если α_j определяются так, как выше, а параметр s после этого выбирается так, чтобы удовлетворялось равенство $\mu'(s)=d/n$.

Интересно сравнить эти оптимальные параметры α_i с теми, которые были найдены в § 13.9 для декодирования максимального правдоподобия, т. е. с

$$\alpha_j=\log_e\left(\frac{p_{cj}}{p_{ej}}\right)\Big/\log_e\left(\frac{p_{cj}}{p_{ej}}\right). \tag{13.68}$$

Хотя оба эти определения совпадают, когда $J=1$ (и $p_c>1/2$), обычно они различны, что отражает различие этих двух правил декодирования (и то, что α_j здесь выбираются так, чтобы минимизировать границу для P_e, а не P_e).

Когда $J=1$ и $p_c\geqslant 1-(d/2n)$, граница (13.61) принимает вид

$$P_e\leqslant\exp\left\{-n\left[\left(1-\frac{d}{2n}\right)\log_e\left(\frac{1-d/2n}{p_c}\right)+\frac{d}{2n}\log_e\left(\frac{d/2n}{1-p_c}\right)\right]\right\} \tag{13.69}$$

и является экспоненциально убывающей функцией n для всех $p_c>1-(d/2n)$. Так как математическое ожидание числа ошибок в

n принятых символах равно $n(1-p_c)$, то условие экспоненциального убывания границы для вероятности ошибки является просто условием того, что математическое ожидание числа ошибок в символах меньше, чем $d/2$; это, очевидно, необходимо и достаточно для того, чтобы вероятность ошибки была мала. В общем случае граница теоремы 13.23, как можно показать, является экспоненциально наиболее точной; никакая граница вида $P_e \leqslant e^{-cn}$ с $c > \max\limits_{s \geqslant 0}[s(d/2)-\mu(s)]$ неверна для достаточно больших n. Граница (13.64), использованная при получении этого результата, обычно называется границей Чернова.

Соотношение между минимальным расстоянием d для кодового словаря и корректирующими способностями словаря очевидно при рассмотрении границы теоремы 13.23. Ясно, что вероятность ошибочного декодирования монотонно убывает по d, когда решения при декодировании основываются на обобщенном минимальном расстоянии. Однако это не обязательно, когда декодирование осуществляется по максимуму правдоподобия, как показывает пример следующих двух словарей:

$$D_1 = \{0000,\ \ 0011,\ \ 1100,\ \ 1111\};$$
$$D_2 = \{0000,\ \ 0001,\ \ 1110,\ \ 1111\}.$$

Если символы приемника являются двоичными, любое слово из D_1 правильно декодируется по методу максимального правдоподобия с вероятностью 1, если вектор ошибки $\mathbf{e}$ имеет вес нуль; с вероятностью 1/2, если он имеет вес один; с вероятностью 1/4, если он отличен от кодового слова и имеет вес два и декодируется ошибочно во всех остальных случаях. Аналогично любое слово из D_2 декодируется правильно, если $\mathbf{e}=0000$, 0010, 0100 или 1000 и декодируется неправильно в остальных случаях. Таким образом, вероятности ошибочного декодирования для D_1 и D_2 равны $P_1 = 1-(1-p)^4-2p(1-p)^3-p^2(1-p)^2$ и $P_2 = 1-(1-p)^4-3p(1-p)^3$ соответственно, где p — вероятность ошибки в символе, и $P_2 < P_1$ для всех $p < 1/2$. Однако D_1 имеет минимальное расстояние 2, в то время как D_2 имеет минимальное расстояние лишь 1. Общее соотношение между вероятностью ошибочного декодирования и минимальным расстоянием, связанными с кодовым словарем, тем не менее отражается границей теоремы 13.23, границей, которая справедлива для декодирования максимального правдоподобия, равно как и для декодирования по минимальному расстоянию.

Можно получить аналогичные границы, связывающие длину кодового ограничения сверточных кодов с вероятностью ошибочного декодирования. Действительно, если сверточный код декодируется с помощью алгоритма декодирования с обратной связью, то граница теоремы 13.23 без изменения может быть применена для вероятности *первого* ошибочного декодирования, если n отождествить с длиной кодового ограничения, а d с начальным расстоянием рассматриваемого кода. Однако, если будет совершена ошибка, последующие ошибочные декодирования будут много более вероятными. Вместе с тем, если правило декодирования позволяет пересматривать начальные решения, то в дальнейшем первое ошибочное декодирование может быть исправлено и вероятность ошибочного декодирования может оказаться даже меньшей, чем для блокового кода с теми же самыми параметрами.

Тот факт, что вероятность ошибки экспоненциально убывает с ростом длины кодового ограничения сверточного кода n и то, что сложность последовательного декодера почти не зависит от n, когда скорость μ/ν поддерживается постоянной, является основным аргументом в пользу этого метода. Длину кодового ограничения можно увеличить так, что вероятность ошибочного декодирования будет пренебрежимо мала. После этого основным параметром станет вероятность *отказа* при декодировании. Эта возможность появляется вследствие того, что число операций, требуемых для декодирования информационного символа, является случайной величиной. При неблагоприятных условиях декодер не будет способен декодировать символы с той же скоростью, с которой они принимаются, и поэтому должен будет запоминать эти символы до тех пор, пока он сможет до них дойти. Отказ при декодировании происходит тогда, когда объем памяти декодера недостаточен для того, чтобы вместить необработанные принятые символы.

Прежде чем закончить этот параграф, обратим внимание на два предположения, которые были приняты во всех рассмотрениях, но которые не обязательно всегда справедливы. Первое состоит в том, что единственной мерой эффективности кода была вероятность ошибочного декодирования. Как было отмечено в § 13.1, например, для кода может быть важнее *обнаруживать* появление определенных ошибок в принятых символах, а не исправлять эти ошибки. Это, в частности, верно, когда можно затребовать повторение передачи. Если этот случай имеет место, процесс декодирования может проходить так же, как и раньше, но с дополнительным ограничением, состоящим в том, что если декодированное и принятое слова отличаются более чем на заданную величину (какая бы мера для этого не использовалась), то декодированное слово отбрасывается. В этом случае очевидно, что вероятность ошибки не является достаточной характеристикой; ее можно в действительности сделать равной нулю, если просто отбросить все принятые слова. Более осмысленной мерой в этой ситуации могла бы быть вероятность правильного решения.

Вторым предположением, которое подразумевалось при рассмотрении, было то, что искажаемые шумом последовательные выходы приемника были статистически независимыми. При нарушении этого условия может возникнуть несколько альтернатив. Одна из них состоит в том, чтобы переставлять символы нескольких слов и посредством этого разделять символы любого частного слова интервалом, достаточным, чтобы гарантировать независимость воздействующего на них шума. Другой метод предполагает, что шум приводит к появлению пачек ошибок. Известен целый ряд конструкций для кодов, *исправляющих пачки ошибок.* Кроме того, многие обычные коды, исправляющие ошибки, в частности, циклические коды, как можно показать, будут эффективными в каналах с пачками ошибок. Это показывает следующая теорема.

Теорема 13.24. Любой циклический (n, k)-код способен обнаруживать любую пачку ошибок длины[1]), не превосходящей $n-k$, обнаруживать любые две пачки с суммарной длиной, не превосходящей $n-2k+1$, или исправлять любую одиночную пачку длины, не превосходящей $(n-2k+1)/2$.

Эффективными для борьбы с пачками ошибок могут оказаться также коды, определенные над большими алфавитами, в которых каждый кодовый символ представляется несколькими символами канала. Если, например, над $GF(q^l)$ определен код с минимальным расстоянием d, и каждый кодовый символ представляется l q-ичными символами канала, то, чтобы изменить $[(d+1)/2]$ кодовых символов и, следовательно, привести к ошибочному декодированию, пачка шума должна воздействовать, по крайней мере, на $l[(d-3)/2]+2$ символов канала.

13.11. Кодирование для канала с белым гауссовским шумом. Полифазные коды

В предыдущих параграфах этой главы рассматривалась задача кодирования для каналов, которые были существенно *симметричными*. Вероятность того, что какой-либо символ будет перепутан с другим, считалась независимой от обоих рассматриваемых символов или, по крайней мере, такой, что качество любого заданного кода могло быть оценено с помощью минимального хэмминговского расстояния между любыми двумя его словами. Эта модель справедлива, например, когда кодовые слова представляются ортогональными функциями с равной энергией и равной длительностью по времени.

Во многих случаях, конечно, такая модель канала не применима. Исследование одной из таких ситуаций составляет предмет настоящего параграфа. А именно, требуется построить N-символьный алфавит для использования в канале с белым гауссовским шумом, соединяя определенным образом элементы r-чных ФТ сигналов:

$$\sqrt{2}\sin\left(\omega_c t+\frac{2\pi x_\nu}{r}\right);\quad iT_s<t<(i+1)\,T_s, \tag{13.70}$$

где $\omega_c=k\pi/T_s$, а k либо равно целому числу, либо велико по сравнению с единицей, и где x_ν — целое число, $0\leqslant x_\nu\leqslant r-1$ (ср. с гл. 4). Сами символы при этом принимают вид

---

[1]) *Длиной* пачки ошибок называется число символов, разделяющих первый и последний кодовые символы, искаженные пачкой (включая сами эти символы). Символы, лежащие внутри, могут быть, а могут и не быть ошибочными. (*Прим. авт.*).

$$x_l(t) = \sqrt{2}\sin\left(\omega_c t + \frac{2\pi\, x_\nu^l}{r}\right) \tag{13.71}$$

при $(\nu-1)T_s < t < \nu T_s$, $\nu = 1, 2, \ldots, n$ с $x_\nu^l \in \{0, 1, \ldots, r-1\}$. (В общем случае, конечно, N будет меньше, чем r^n, так что некоторые последовательности не будут представлять собой символы. Преимущество такого типа конструкции символов станет вскоре очевидным.)

Если требуется, чтобы принятый сигнал был демодулирован когерентно (см. § 4.2), то вероятность ошибки, связанная с таким множеством сигналов, при заданном отношении сигнал/шум является функцией лишь нормированных коэффициентов корреляции:

$$\widetilde{\rho}_{lm} = \frac{1}{nT_s}\int\limits_0^{nT_s} x_l(t)\, x_m(t)\, dt = \frac{1}{n}\sum_{\nu=1}^{n}\cos\frac{2\pi}{r}\left(x_\nu^l - x_\nu^m\right) =$$

$$= \operatorname{Re}\left\{\frac{1}{n}\sum_{\nu=1}^{n} \mathrm{e}^{(2\pi \mathrm{i}/r)\left(x_\nu^l - \nu_\nu^m\right)}\right\}, \tag{13.72}$$

где $\operatorname{Re}(z)$ обозначает действительную часть z. Для случая некогерентной демодуляции (см. § 4.3) параметры

$$\hat{\rho}_{lm} = \frac{1}{nT_s}\int\limits_0^{nT_s} x_l(t)\, \hat{x}_m(t) dt = \frac{1}{n}\sum_{\nu=1}^{n}\sin\frac{2\pi}{r}\left(x_\nu^l - x_\nu^m\right) =$$

$$= \operatorname{Im}\left\{\frac{1}{n}\sum_{\nu=1}^{n} \mathrm{e}^{(2\pi \mathrm{i}/r)\left(x_\nu^l - x_\nu^{(m)}\right)}\right\} \tag{13.73}$$

также имеют важное значение. Здесь $\hat{x}_m(t) = \sqrt{2}\cos[\omega_c t + (2\pi x_\nu^m/r)]$; $(\nu-1)T_s < t < \nu T_s$ и $\operatorname{Im}(z)$ — мнимая часть комплексной переменной z. В обоих случаях сумма $\frac{1}{n}\sum\limits_{\nu=1}^{n} \mathrm{e}^{(2\pi \mathrm{i}/r)\left(x_\nu^l - x_\nu^m\right)}$ является мерой, которая представляет интерес[1]).

Поставленная задача может, таким образом, быть рассмотрена как задача кодирования, в которой кодовые символы являются элементами из множества $\{\zeta(\nu)\} \triangleq \{\exp(2\pi \mathrm{i}\nu/r)\}$. Цель состоит в том, чтобы составить из этих символов N кодовых слов длины n: $\zeta^l = \{\zeta(x^l_1), \zeta(x^l_2), \ldots, \zeta(x^l_n)\}$, причем эффективность любого заданного кодирования измеряется с помощью скалярных произведений $\zeta^l \cdot \zeta^m$, $l \neq m$ [ср. с (13.72) и (13.73)]. Такие коды будут называться *полифазными* или, более просто, *фазовыми* кодами.

Удобно ввести структуру в множество n-последовательностей $\mathbf{x}^\alpha = (x^\alpha_1, x^\alpha_2, \ldots, x^\alpha_n)$, состоящее из показателей степеней слов фазового кода. В частности, предположим, что множество $G=\{\mathbf{x}^\alpha\}$ образует абелеву группу относительно операций покомпонентного сложения по модулю r, т. е. $\mathbf{x}^\alpha+\mathbf{x}^\beta=(x^\alpha{}_1+x^\beta{}_1,\ x^\alpha{}_2+x^\beta{}_2,\ \ldots,\ x^\alpha{}_n+{}$ $+x^\beta{}_n)$. Получающийся фазовый код называется *групповым* кодом, а G — кодовой *степенной группой*[1]. (Отметим, что если r простое, то G также является векторным пространством.) Тогда все коэффициенты корреляции (13.72) и (13.73) содержатся в множестве

---

[1]) Связанной с ней мерой, которая приводит к некоторым интересным кодам, является *метрика Ли. (Прим. авт.).*

$$\rho_\alpha=\frac{1}{n}\sum_{\nu=1}^{n}\mathrm{e}^{(2\pi\mathrm{i}/r)x^\alpha_\nu},\quad \alpha=1,\ 2,\ \ldots,\ N. \tag{13.74}$$

Так же как и в случае кодов, исправляющих ошибки, наличие структуры упрощает задачу определения «хороших» кодов. Фазовый код, конечно, описывается не с помощью его весовой структуры, а с помощью множества параметров ρ_α, которые определены соотношением (13.74)[2].

Теорема 13.25. Пусть $\xi^\alpha=(\xi^\alpha{}_1,\ \xi^\alpha{}_2,\ \ldots,\ \xi^\alpha{}_n)$, $\alpha=1,\ 2,\ \ldots,\ N$ являются N n-компонентными векторами, определенными над полем комплексных чисел и пусть

$$\rho_{\alpha\beta}=\frac{1}{n}\ \xi^\alpha\cdot\xi^\beta=\frac{1}{n}\sum_{\nu=1}^{n}\xi^\alpha_\nu(\xi^\beta_\nu)^*,$$

где $\rho_{\alpha\alpha}=1$ для всех α и где $(\xi^\alpha_\nu)^*$ — комплексно-сопряженная величина. Пусть далее $\tilde\rho_{\alpha\beta}=\mathrm{Re}(\rho_{\alpha\beta})$ и $\hat\rho_{\alpha\beta}$ $\mathrm{Im}(\rho_{\alpha\beta})$. Тогда

1. Если $\tilde\rho_{\alpha\beta}=0$ для всех $\alpha\neq\beta$, то $N\leqslant n$.
2. Если $\tilde\rho_{\alpha\beta}=-1/n$ для всех $\alpha\neq\beta$, то $N\leqslant n+1$.
3. Если $\hat\rho_{\alpha\beta}=0$ для всех $\alpha\neq\beta$, то $N\leqslant 2n$.
4. Существуют фазовые коды, содержащие N n-символьных слов, для всех n, удовлетворяющих ограничениям 1, 2 и 3, такие, что в каждом из случаев N равно соответствующей верхней границе.

Доказательство. Утверждение *1*. Пространство V, содержащее n-компонентные векторы ξ^α, принадлежит пространству n-последовательностей над полем комплексных чисел и, следовательно, имеет максимальную размерность n. Это значит, что максимальное число линейно независимых векторов в V равно n. Но если множество векторов $\{\xi^\alpha\}$ удовлетворяет условиям $\rho_{\alpha\beta}=0$ для всех $\alpha\neq\beta$, то, очевидно, они являются линейно независимыми. Максимальное число векторов, удовлетворяющих утверждению *1*, равно поэтому n, и утверждение доказано.

---

[1] Сам фазовый кодовый словарь является группой n-последовательностей относительно операций покомпонентного *умножения*. Однако обычно более удобно описывать код с помощью степеней этих последовательностей. (*Прим. авт.*).

[2] Заметим, что, когда $r=2$, то $\rho_\alpha=(n-2d_\alpha)/n$, где d_α — хэмминговский вес n-последовательности $\mathbf{x}^\alpha$. Так как двоичное векторное пространство также образует группу то все двоичные коды, рассмотренные в предыдущих параграфах, можно использовать для определения фазовых кодов. То же самое можно сказать о соответствии между словарем троичного кода, исправляющего ошибки, и троичного фазового кода в случае фазовокогерентного приема. Так, в этом случае $\tilde\rho_\alpha=(n-d_\alpha)/n$, где d_α определено ранее. (*Прим. авт.*).

Утверждение *2*. Предположим, что n-компонентные векторы ξ^α удовлетворяют утверждению *2*. Тогда корреляция $\rho'_{\alpha\beta}$ между векторами η^α и η^β, где $\eta^l=(1, \xi^l_1, \xi^l_2, \ldots, \xi^l_n)$, равна $\rho'_{\alpha\beta}=1/(n+1)+n/(n+1)(-1/n)=0$ для всех $\alpha\neq\beta$. Таким образом, согласно утверждению *1* $N\leqslant n+1$.

Утверждение *3*. Предположим, что N векторов ξ^α удовлетворяют утверждению *3*, и определим $2n$-компонентные векторы

$$\eta^\alpha=\{\xi^\alpha,(\xi^\alpha)^*\}=\{\xi_1^\alpha,\ \xi_2^\alpha,\ \ldots,\ \xi_n^\alpha,\ (\xi_1^\alpha)^*,\ (\xi_2^\alpha)^*,\ \ldots,\ (\xi_n^\alpha)^*\}.$$

Тогда

$$\frac{1}{2n}\eta^\alpha\cdot\eta^\beta=\frac{1}{2n}\{\xi^\alpha\cdot\xi^\beta+(\xi^\alpha\cdot\xi^\beta)^*\}=\frac{1}{n}\mathrm{Re}\{\xi^\alpha\cdot\xi^\beta\}=\widetilde{\rho}_{\alpha\beta}=0.$$

Следовательно, утверждение *1* гарантирует максимум $2n$ таких векторов η_α и поэтому максимум $2n$ векторов ξ_α, что и требовалось доказать.

Утверждение *4*. Пусть D_0 — словарь, определяемый степенной группой G_0, содержащей все кратные по модулю r r-последовательности $(0, 1, 2, \ldots, r-1)$. Тогда корреляция между любыми двумя различными словами из D_0

$$\rho_{\alpha\beta}=\frac{1}{r}\sum_{\nu=0}^{r-1}e^{(2\pi i/r)(\alpha-\beta)\nu}=0$$

для всех $\alpha\neq\beta$. Так как словарь D_0 содержит r слов по r символов в каждом, то он лежит на границе, указанной в утверждении *1*. Аналогично, если G_1 — группа $(r-1)$-последовательностей, образуемая при опускании первого нуля из каждого элемента в G_0, то $\rho_{\alpha\beta}=-1/(r-1)$, $\alpha\neq\beta$ и, соответствующий словарь D_1 лежит на границе *2*. Наконец, словарь $D_2=D_1\cup(iD_1)$ (где iD_1 — словарь, образуемый умножением каждого символа из D на i) содержит $2n$ слов с $\widetilde{\rho}_{\alpha\beta}=0$, $\alpha\neq\beta$ и, следовательно, лежит на границе *3*. Это завершает доказательство теоремы.

Словари, лежащие на границе, задаваемой утверждением *1*, называются *ортогональными;* лежащие на границе, задаваемой утверждением *2*, называются *трансортогональными*, а лежащие на границе, задаваемой утверждением *3*, *ортогональными в фазово-когерентном смысле.*

Теорема 13.26. Пусть **A** и **B** матрицы размеров $M\times m$ и $N\times n$, строки которых являются словами групповых фазовых кодов A и B соответственно. Пусть $S_A=\{\rho_\alpha(A)\}$ — множество коэффициентов корреляции между любыми парами слов из A, а $S_B=$

$=\{\rho_\beta(B)\}$ — аналогичное множество для B. Если $\mathbf{C}=\mathbf{A}\times\mathbf{B}$ является кронекеровским произведением $\mathbf{A}$ и $\mathbf{B}$, то строки $\mathbf{C}$ образуют групповой фазовый код C из MN mn-символьных слов, и если $S_C=\{\rho_\alpha(C)\}$ — множество коэффициентов корреляции, связанных с C, то $\rho_\gamma(C)=\rho_\alpha(A)\rho_\beta(B)$, где $\gamma=\alpha N+\beta$ относится к γ-й строке матрицы $\mathbf{C}$, α к α-й, а β к β-й строке $\mathbf{A}$ и $\mathbf{B}$ соответственно.

Доказательство. То, что строки $\mathbf{C}=\mathbf{A}\times\mathbf{B}$ образуют группу, следует из эквивалентности кронекеровского произведения матриц фазового кода и кронекеровской суммы, связанной со степенными матрицами. Кронекеровская сумма двух групп, как легко проверить, сама является группой.

В соответствии с этим множество коэффициентов корреляции C является множеством $\{\rho_\gamma(C)\}$, где

$$\rho_\gamma(C)=\frac{1}{mn}\sum_{\nu=1}^{mn} e^{(2\pi i/r) z^{\gamma}_{\nu}} \qquad (13.75)$$

и где $(z^{\gamma}_{1}, z^{\gamma}_{2}, \ldots, z^{\gamma}_{mn})$ — элемент степенной группы, соответствующий γ-й строке $\mathbf{C}$. Но если $\gamma=\alpha N+\beta$, то

$$\frac{1}{mn}\sum_{\nu=1}^{mn} e^{(2\pi i/r) z^{\gamma}_{\nu}}=\frac{1}{mn}\sum_{\mu=1}^{m}\sum_{\nu=1}^{n} e^{(2\pi i/r)\left(y^{\beta}_{\nu}+x^{\alpha}_{\mu}\right)}=$$

$$=\left(\frac{1}{m}\sum_{\mu=1}^{m} e^{(2\pi i/r) x^{\alpha}_{\mu}}\right)\left(\frac{1}{n}\sum_{\nu=1}^{n} e^{(2\pi i/r) y^{\beta}_{\nu}}\right), \qquad (13.76)$$

где $(x^{\alpha}_{1}, x^{\alpha}_{2}, \ldots, x^{\alpha}_{m})$ и $(y^{\beta}_{1}, y^{\beta}_{2}, \ldots, y^{\beta}_{n})$ являются элементами степенных групп, соответствующих α- и β-й строкам $\mathbf{A}$ и $\mathbf{B}$. Таким образом, $\rho_\alpha(C)=\rho_\gamma(A)\rho_\beta(B)$, и теорема доказана.

Следствие. Получаемый с помощью кронекеровского произведения ортогонального $(r, 1)$-словаря на самого себя k раз, (r^k, k)-словарь (т. е. словарь $n=r^k$, $N=r^k$) также является ортогональным словарем.

Доказательство сразу же следует из теоремы 13.26, так как либо $\rho_\alpha(A)=0$ или $\rho_\beta(B)=0$, либо справедливы оба равенства для любого $\gamma=\alpha N+\beta\neq 0$.

Следствие. Трансортогональные фазовые $(r^k—1, k)$-коды существуют для всех r и k и могут быть получены отбрасыванием первой компоненты из каждого слова соответствующим образом выбранных ортогональных словарей.

Доказательство. Первая компонента каждого из слов ортогонального $(r, 1)$-словаря, как указывалось при доказательстве теоремы 13.25, равна 1. Это свойство, очевидно, сохраняется для кронекеровского произведения любых двух таких словарей. Таким образом, опуская этот первый символ из каждого слова, получаем $\rho'_\gamma=(N\rho-1)/(N-1)$, что и требовалось доказать.

Как упомянуто в гл. 4, трансортогональные коды, по-видимому, оптимальны для фазовокогерентных (а ортогональные коды для фазовонекогерентных) каналов с белым гауссовским шумом. В силу того что N-словный бифазный (0 и 180°) ортогональный и трансортогональный, а также $2N$-словный четырехфазный (0, 90, 180 и 270°) фазовокогерентный ортогональный словари существуют для всех $N=2^k$, возможное преимущество других методов кодирования ставится под вопрос. Но если информация переносится фазовым кодом, содержащим N n-символьных слов, то каждый бит информации представляется $n/\log_2 N$ кодовыми символами. Если фиксирована скорость передачи информации, то требуемая полоса увеличивается по сравнению с полосой при передаче той же информации при использовании двоичного кодирования во столько же раз. Ортогональные (и трансортогональные) коды могут поэтому быть использованы только в случае, когда коэффициент расширения полосы $n/\log_2 n$ является допустимым. Очевидно, что это накладывает ограничение на допустимую длину кодового слова. Однако, как было показано в гл. 4, вероятность ошибки экспоненциально убывает с ростом n, даже когда $\rho_{\text{макс}}$ (или $|\rho_{\text{макс}}|$) больше нуля. Это означает, что когда ограничена полоса частот, может оказаться целесообразным использование отличных от ортогональных кодов, которые имеют бо́льшие коэффициенты корреляции, но зато меньший коэффициент расширения полосы частот. Этот обмен выгоден, конечно, если длина слова n может быть увеличена настолько, чтобы компенсировать увеличение коэффициентов корреляции, не нарушая ограничения на ширину полосы частот. Хотя относительно того, как произвести наиболее выгодный обмен, известно, в общем, немного, методы фазового кодирования были использованы для этой цели с некоторым успехом.

Один из методов увеличения числа слов в фазовом кодовом словаре при фиксированной длине слова состоит в следующем. Пусть G — степенна́я группа ортогонального фазового кода; присоединим к G ее *смежные классы* $C_1, C_2, \ldots, C_{r-1}$, где C_ν обозначает смежный класс G, содержащий n-последовательность $(\nu, \nu, \ldots \ldots, \nu)$. Число слов в соответствующем словаре фазового кода увеличивается благодаря этому в r раз. Корреляция между степенью любого слова из C_ν и степенью любого слова из C_μ

$$\rho_{\mu\nu} = \frac{1}{n} \sum_{i=1}^{n} e^{(2\pi i/r)\left(x_l^\alpha - x_l^\beta\right)} e^{(2\pi i/r)(\nu-\mu)}, \tag{13.77}$$

где $\mathbf{x}^\alpha$ и $\mathbf{x}^\beta$ — n-последовательности из G. Таким образом,

$$\rho_{\nu\mu} = \begin{cases} 0, & \alpha \neq \beta; \\ e^{(2\pi i/r)(\nu-\mu)}, & \alpha = \beta \end{cases}$$

и $\max\limits_{\nu\neq\mu} \widetilde{\rho}_{\nu\mu} = \cos(2\pi/r), \quad r > 3.$

Когда $r=2$, число слов в словаре просто удваивается за счет включения в него также отрицательных значений этих слов. Это, разумеется, дает *биортогональный* словарь (см. § 4.2). По аналогии для произвольного значения r такие словари будем называть *r-ортогональными* словарями. Тот же метод, между прочим, может быть использован для увеличения объема кода даже тогда, когда основной ортогональный код не является фазовым кодом (например, когда он является множеством ЧТ символов) или когда степени фазового кода определяются по модулю, отличному от того значения r, которое используется в определении смежных классов. Однако довольно часто возможно убедительное уменьшение сложности оборудования, если для получения требуемого множества сигналов используются групповые фазовые коды, в отличие, например, от ЧТ методов. Информация может кодироваться так, как если бы она должна была передаваться по r-ичному симметричному каналу, а получающаяся последовательность r-ичных символов использоваться для фазовой модуляции синусоиды. Кодер может иметь вид, изображенный на рис. 13.1.

Например, как легко понять (см. теорему 13.26), степенная группа двоичного биортогонального $(2^{k-1}, k)$-кода состоит из 2^k линейных комбинаций над двоичным полем, составленных из k 2^{k-1}-последовательностей [1]:

$$\begin{array}{lcl}
111111111 & \ldots\ldots\ldots\ldots & 11 \\
010101010 & \ldots\ldots\ldots\ldots & 01 \\
001100110 & \ldots\ldots\ldots\ldots & 11 \\
\ldots\ldots\ldots & \ldots\ldots\ldots\ldots & . \\
000000000 & \ldots\ldots\ldots\ldots & 11,
\end{array} \tag{13.78}$$

т. е. из двоичных последовательностей с периодами 1, 2, 4, 8, ..., 2^{k-1}. Запоминающие устройства в схеме 13.1 могут поэтому быть заменены в этом случае k-разрядным двоичным счетчиком. Выходы последовательных разрядов такого счетчика представляют собой точно требуемые последовательности. Соответствующий биортогональный код, следовательно, генерируется особенно просто.

Реализация приемника может быть также значительно упрощена при использовании фазовых кодов вследствие того, что если $y(t)$ — принятый искаженный шумом сигнал вида (13.71), то корреляция между ним и l-м кодовым словом равна

$$\frac{1}{n}\sum_{\nu=1}^{n} \xi_\nu^l \eta_\nu, \tag{13.79}$$

где $\xi_\nu^l = e^{(2\pi i/r)x_\nu^l}$; x_ν^l обозначает фазу l-го кодового слова на интервале $(\nu-1)T_s < t < \nu T_s$ и где

$$\eta_\nu = \frac{1}{T_s}\int_{(\nu-1)T_s}^{\nu T_s} y(t)\sin\omega_c t\,dt = \frac{i}{T_s}\int_{(\nu-1)T_s}^{\nu T_s} y(t)\cos\omega_c t\,dt.$$

---

[1] Заметим, что эти векторы порождают $(2^{k-1}, k)$-код Рида—Маллера, определенный в § 13.8. *(Прим. авт.)*.

Необходимо лишь определить величины η_ν, выполнить матричную операцию

$$\mathbf{M}\mathbf{y} = \mathbf{z}, \tag{13.80}$$

где $\mathbf{M}$ — $N\times n$-матрица $\{\xi_\nu^l\}$, $l=1, 2, \ldots, N$, $\nu=1, 2, \ldots, n$, а $\mathbf{y}=(\eta_1, \eta_2, \ldots, \eta_n)^T$. Компонента $\mathbf{z}$, имеющая наибольшую действительную часть (или в случае фазовонекогерентного приема, имеющая наибольшее абсолютное значение), указывает тогда наиболее вероятно принятое слово. Матричное умножение можно выполнить численно с помощью специализированной или универсальной ЦВМ. Известны особенно эффективные алгоритмы для выполнения этого умножения, когда кодовый словарь является кронекеровским произведением словарей.

Вероятности ошибок, связанные с ортогональным, биортогональным и трансортогональным множествами сигналов, были уже исследованы в гл. 4. Конечно, границы, полученные в этой главе, можно применить к любому фазовому коду, когда шум является аддитивным белым и гауссовским.

Глава 14

СИНХРОНИЗИРУЕМЫЕ КОДЫ, ИСПРАВЛЯЮЩИЕ ОШИБКИ

14.1. Введение

Коды, исправляющие ошибки, так же как и менее избыточные коды, рассмотренные в гл. 10, имеют значительно большую практическую ценность в случае, когда они являются также синхронизируемыми. Так как слова в кодах, исправляющих ошибки, обычно все имеют одну и ту же длину, то они обязательно однозначно декодируемы. Но они редко являются синхронизируемыми без какого-либо изменения; все линейные коды, например, содержат чисто нулевое кодовое слово. Изменение кодов, исправляющих ошибки с целью сделать их синхронизируемыми, является предметом этой главы.

Как впервые было указано в гл. 11, термин синхронизируемый словарь применялся к таким словарям, для которых декодер может определить синхронизацию слов непосредственно по принятому потоку символов в отсутствие какой-либо дополнительной информации относительно этой синхронизации и после того, как будет принято лишь конечное число символов. Это определение, конечно, должно быть дополнено словами «в отсутствие ошибок в символах» (или, по крайней мере, «в отсутствие определенных комбинаций ошибок») для того, чтобы оно было полезным для каналов с шумами, так как неудачно расположенные ошибки в символах, очевидно, могли бы бесконечно задержать синхронизацию слов независимо от того, какой код используется. На самом деле из-за возможности ошибок в символах первоначальная синхронизируемость может оказаться недостаточной для кодов, которые нужно использовать в каналах с шумами. Тем не менее требование синхронизируемости накладывает такие ограничения на принимаемую последовательность символов, что, по-видимому, правильная синхронизация может быть получена после достаточно длинного периода наблюдения даже в присутствии ошибок. Этот вопрос будет в дальнейшем разобран детально (см. § 14.5). Первые несколько параграфов этой главы посвящены методам изменения кодов, исправляющих ошибки, для превращения их в синхронизируемые в первоначальном смысле. Это исследование имеет дополнительную цель создать фундамент для материала дальнейших параграфов, в которых этот подход будет обобщен и видоизменен.

Хотя в этой главе явно не будут исследованы возможные синхронизационные свойства сверточных кодов, упомянем, что, по крайней мере, некоторые методы, которые рассматриваются здесь, легко обобщить также и на эти коды. Это, очевидно, верно, когда (как это часто делается) закодированная последовательность символов периодически обрывается (см. § 13.8) и поэтому превращается в блоковый код некоторой (в общем, большой) блоковой длины N. Однако независимо от того, обрывается код или нет, декодер должен, по крайней мере, быть способен разделять принятую последовательность на ν-символьные отрезки, соответствующие μ-символьным блокам информационных символов, поступающим на вход кодера. (Терминологию см. в § 13.8.) Иногда эта задача называется задачей синхронизации *узлов* или *ребер*. Одним из методов ее решения является такое рассмотрение закодированного потока символов, как будто бы он представляет собой последовательность слов линейного блокового $(\nu, m\mu)$-кода. (Конечно, при этом не учитывается зависимость между последовательными ν-символьными отрезками, которая вводится структурой сверточного кода.) Методы, которые разработаны в этой главе для того, чтобы декодер получил возможность отличать правильные (блоковые) кодовые слова от стыков слов, можно будет затем непосредственно применять и использовать для того, чтобы снабдить сверточные коды дополнительной структурой, необходимой для установления более легкой синхронизации узлов. Как будет показано, эффективность этих методов обычно является убывающей функцией скорости передачи информации. Поэтому в действительности может оказаться выгодным рассматривать последовательность принятых символов как последовательность слов блокового $(i\nu, (m+i-1)\mu)$-кода для некоторого целого $i>1$ и посредством этого использовать кодовую структуру более эффективно. Будет ли результирующее уменьшение времени синхронизации вызывать приемлемое сопутствующее увеличение сложности синхронизатора, зависит, однако, как от кода, так и от параметров канала. В любом случае применимость для синхронизации узлов методов, рассматриваемых ниже, должна быть очевидной.

14.2. Префиксные коды и коды с запятой, исправляющие ошибки

Одним из методов для превращения блоковых кодов в синхронизируемые, исследованных в гл. 12, было приписывание в качестве префикса каждому слову некоторой l-последовательности, такой, чтобы эта l-последовательность нигде не появлялась в любой последовательности кодовых слов. Второй метод состоял в периодической передаче запятой в последовательности кодовых слов; словарь при этом выбирался так, чтобы гарантировать то, что эта запятая не появилась во всех случаях, кроме того, когда она специально передается. Эти два метода применяются и здесь к кодовым словарям, исправляющим ошибки.

Каждая из q^k различных k-последовательностей появляется в качестве начальных k символов некоторого слова в любом *систе-*

матическом q-ичном (n, k)-кодовом словаре. В равной мере это утверждение применимо к любому смежному классу систематического кода. Следовательно, если q^k-словный код является систематическим (и часто даже, если он не является таковым), то любой префикс для того, чтобы он был единственным, должен содержать, по меньшей мере, $k+1$ символов. Присоединяя такой префикс к каждому слову, получаем, следовательно, увеличение его избыточности, по меньшей мере, на $k+1$ символов без какого-либо улучшения свойств расстояния в коде. Если k мало по сравнению с n, этот метод может быть удобным, но если k увеличивается, то эта добавочная избыточность становится более серьезной проблемой. Тем не менее следующая теорема гарантирует существование простого метода, посредством которого любой циклический код может быть сделан синхронизируемым с помощью легко реализуемой процедуры синхронизации.

Теорема 14.1. Любой циклический (n, k)-код можно превратить в префиксный код, если перед каждым словом поставить префикс $000\ldots0a$, состоящий из k нулей, за которыми следует какой-либо ненулевой символ алфавита. Никакой более короткий префикс для этой цели использовать нельзя.

Доказательство. Так как префикс $00\ldots0a$ не имеет другого периода повторения, кроме $k+1$ (см. § 12.4), то никакое стыковое слово, образуемое двумя словами снабженного префиксом кода, не может содержать этот префикс. В силу того что первоначальный код систематический, $k+1$-й и последующие символы определяются с помощью проверок для первых k символов. Если первые k символов нулевые, то таким же должен быть и $k+1$-й символ. Так как код циклический, то за всеми последовательностями из k последовательных нулей должен следовать нуль. Следовательно, комбинация $000\ldots0a$ может возникнуть только на месте префикса и никогда не может возникнуть в другом месте, и расширенный код (т. е. код, получающийся, когда каждому слову предшествует рассматриваемый префикс) является префиксным кодом. То, что никакой более короткий префикс не может быть использован, чтобы получить это свойство, было уже доказано. (Заметим, что этот результат справедлив, даже если $k=n$).

Расширенный код, конечно, не является больше линейным. Однако это не существенно, так как префикс используется только для синхронизации принимаемой последовательности слов; он может не учитываться при операциях кодирования и декодирования, и преимущества линейных кодов все еще можно использовать.

Более слабый результат можно получить для линейных кодов в общем случае, заметив, что, если код имеет минимальное хэмминговское расстояние d, то все кодовые слова (кроме чисто нулевого слова) имеют, по меньшей мере, d ненулевых элементов. Длина самой длинной серии нулей в любом (кроме чисто нулевого) кодовом слове поэтому не может быть больше $n-d$. Это утверждает следующая теорема.

Теорема 14.2. Любой линейный кодовый словарь с n-символьными словами и минимальным расстоянием d можно превратить в префиксный код, добавляя к каждому кодовому слову префикс $000\ldots0a$ длины $n-d+2$, где a — какой-либо ненулевой символ алфавита.

Так как для любого линейного кода $n-d+2 \geqslant k+1$ (см. § 13.4), то этот метод всегда менее эффективен, чем тот, который описан для циклических кодов.

Другой метод для синхронизации блоковых кодов, рассмотренный в гл. 13, состоял в периодической передаче m-символьной *запятой*. Любая запятая, которая должна быть сингулярной по отношению к циклическому (n, k)-коду, должна иметь длину, по меньшей мере, $2k+1$. Это следует из того, что каждая k-последовательность может появляться как в начале некоторого кодового слова, так и в конце его. Стыковые слова должны поэтому содержать любую возможную $2k$-последовательность.

Теорема 14.3. Существует запятая длины $2k+1$, которая является сингулярной по отношению к любому циклическому (n, k)-коду при всех n и k, $k \leqslant n-1$. Никакая более короткая запятая не обладает этим свойством.

Доказательство. Последнее утверждение уже было доказано. (Между прочим, это утверждение в равной мере применимо к любому смежному классу циклического кода.) Существование сингулярной запятой длины $2k+1$ становится ясным при рассмотрении запятой $0000\ldots0a\ 0\ldots0$, состоящей из k нулей, за которыми следует какой-либо ненулевой символ алфавита и еще k нулей. Чтобы доказать, что эта запятая сингулярна, заметим, что, во-первых, никакая перестановка n-последовательности $x=000\ldots0a$ не является кодовым словом и, во-вторых, никакая из двух $(k+1)$-последовательностей $s_1=000\ldots0a$ и $s_2=a00\ldots0$ не появляется ни в каком кодовом слове. Оба утверждения немедленно следуют из того, что в циклическом коде никакое слово, кроме чисто нулевого слова, не содержит последовательности, состоящей из более чем $k-1$ последовательных нулей. Но для того, чтобы стык двух или большего числа кодовых слов образовал запятую, какое-либо одно из слов должно содержать s_1 или s_2 или должно совпадать с некоторой циклической перестановкой x. Никакая из этих ситуаций невозможна. Аналогично для того, чтобы некоторый стык, в котором участвуют как кодовые слова, так и запятая, образовал запятую, по меньшей мере, $k+1$ символов этой запятой должны быть внесены одним кодовым словом; опять-таки это кодовое слово должно было бы содержать либо s_1, либо s_2 или быть некоторой перестановкой x, и, следовательно, оно не существует. Это доказывает теорему.

Другим методом построения кода с запятой, обладающего также способностью исправлять ошибки, является тот, который определяется теоремой.

Теорема 14.4. Пусть D — любой циклический (n, k)-кодовый словарь, исправляющий ошибки, и пусть D' — словарь, получаемый выбрасыванием из D чисто нулевого кодового слова. Тогда запятая $000\ldots0a$, состоящая из $2k-1$ нулей, за которыми следует какой-либо ненулевой элемент, является сингулярной по отношению к D'.

Доказательство. Никакое слово из D' не может содержать нулевую k-последовательность. Однако для того, чтобы какой-нибудь стык кодовых слов образовал запятую, одно из слов должно содержать нулевую k-последовательность. Очевидно, что никакой стык, содержащий запятую, не может образовывать запятую, и теорема доказана. (Нет необходимости здесь требовать, чтобы $k<n$; см. § 12.5.) ■

Так же, как и в случае линейных префиксных кодов, можно доказать отчасти более слабый результат для произвольных линейных кодов с запятой.

Теорема 14.5. Запятая $000\ldots0a$ длины $2(n-d)+2$ сингулярна по отношению к любому линейному словарю, содержащему n-символьные слова, разделенные минимальным расстоянием d, из которого удалено нулевое слово.

Доказательство. Так как самая длинная последовательность из нулей, образующаяся из стыка двух слов, имеет длину $2(n-d)$ (если последние $n-d$ символов одного слова и первые $n-d$ символов второго слова являются чисто нулевыми), то $2(n-d)+1$ нулей будут отмечать присутствие запятой, конец которой указывается символом a.

14.3. Коды без запятой, исправляющие ошибки

Одно из ограничений, которое полезно, как было показано, наложить на блоковые коды, состояло в требовании «свободы от запятой». Используя лишь около $1/n$ общего числа имеющихся в распоряжении n-последовательностей, можно добиться того, что все возможные стыки кодовых слов будут принадлежать множеству исключенных n-последовательностей. Так как коды, исправляющие ошибки, также используют в качестве кодовых слов лишь подмножество всех n-последовательностей, можно было бы надеяться, что выбрасывание нескольких дополнительных n-последовательностей превратит его в код без запятой. В § 14.4 будет доказано, что, действительно, по крайней мере, когда код циклический и достаточно избыточный, некоторые из его смежных классов будут кодами без запятой. Таким образом, он может быть очень просто превращен в код без запятой без *какого-либо* дополнительного исключения n-последовательностей из словаря и без потери каких-либо алгебраических свойств, которые полезны для кодирования и декодирования. В этом параграфе дано довольно простое правило определения того, существует или нет смежный класс линейного кода, который является кодом без запятой.

Код будет называться *неуязвимым при синхронизации на m-й позиции,* если последовательность

$$b_{m+1}b_{m+2}\ldots b_n\, a_1a_2\ldots a_m \qquad (14.1)$$

не является кодовым словом, где $a_1a_2\ldots a_n$ и $b_1b_2,\ldots,b_n$ — какие-либо два (не обязательно различных) слова из кода. Если код неуязвим на всех m позициях ($m=1, 2, \ldots, n-1$), то, конечно, он является кодом без запятой. Если код линейный, то, очевидно, что он не является неуязвимым ни на какой позиции, так как он должен содержать слово $00\ldots0$. Однако можно прибавить вектор $\mathbf{c}$ к каждому кодовому слову для того, чтобы сформировать смежный класс, который является неуязвимым, по крайней мере, на некоторых позициях. Смежный класс обладает теми же самыми свойствами исправлять ошибки, что и первоначальный код, так как он имеет те же самые расстояния.

Пусть $\mathbf{G}$ $k\times n$-матрица, строки которой являются порождающими векторами подпространства над $GF(q)$. Тогда любой вектор из подпространства (рассматриваемый как вектор-строка) можно представить в виде $\mathbf{xG}$, где $\mathbf{x}$ является q-ичной k-компонентной вектор-строкой. Если код является смежным классом подпространства, порождаемого $\mathbf{G}$, то любое кодовое слово $\mathbf{w}$ представляется в виде

$$\mathbf{w}=\mathbf{xG}+\mathbf{c} \qquad (14.2)$$

при некотором векторе $\mathbf{x}$. Пусть теперь $\mathbf{G}$ разбивается на матрицы $\mathbf{G}_1$ и $\mathbf{G}_2$ размеров $k\times m$ и $k\times(n-m)$ соответственно:

$$\mathbf{G}=(\mathbf{G}_1,\ \mathbf{G}_2); \qquad (14.3)$$

аналогично пусть $\mathbf{c}$ разбивается на векторы $\mathbf{c}_1$ и $\mathbf{c}_2$ с m и $n-m$ компонентами в каждом:

$$\mathbf{c}=(\mathbf{c}_1,\ \mathbf{c}_2). \qquad (14.4)$$

Число совпадающих координат в любом кодовом слове и любом стыке слов вида (14.1) может быть теперь определено с помощью подсчета числа нулей в векторе вида

$$\mathbf{xG}+\mathbf{c}-\mathbf{y}(\mathbf{G}_2,\mathbf{0}_m)-\mathbf{z}(\mathbf{0}_{n-m},\ \mathbf{G}_1)-(\mathbf{c}_2,\ \mathbf{c}_1)=$$

$$=[\mathbf{x},\ -\mathbf{y},\ -\mathbf{z}]\begin{bmatrix} \multicolumn{2}{c}{\mathbf{G}} \\ \mathbf{G}_2, & \mathbf{0}_{n-m} \\ \mathbf{0}_m, & \mathbf{G}_1 \end{bmatrix}+\mathbf{c}-[\mathbf{c}_2,\ \mathbf{c}_1]. \qquad (14.5)$$

Матрицы $\mathbf{O}_l$ являются $k\times l$-матрицами, все элементы которых являются нулями, а $\mathbf{x}$, $\mathbf{y}$ и $\mathbf{z}$ — k-компонентные векторы. Если смежный класс, который должен быть использован в качестве словаря, является уязвимым при синхронизации на m-й позиции, то существует некоторый $2k$-мерный q-ичный вектор-столбец $\mathbf{v}$, такой, что

$$\mathbf{Mv}=\mathbf{b}. \qquad (14.6)$$

где $$\mathbf{M} = \begin{bmatrix} & \mathbf{G} \\ \mathbf{G}_2, & \mathbf{0}_{n-m} \\ \mathbf{0}_m, & \mathbf{G}_1 \end{bmatrix}^T; \quad \mathbf{b} = [(\mathbf{c}_2, \ \mathbf{c}_1) - \mathbf{c}]^T.$$

Для того чтобы доказать, что код неуязвим на m-й позиции, достаточно показать, что не существует вектор, для которого написанное выше уравнение имеет решение. Но это уравнение имеет решение тогда и только тогда, когда

$$\rho(\mathbf{M}) = \rho(\mathbf{M}, \ \mathbf{b}), \tag{14.7}$$

где $\rho(\mathbf{A})$ обозначает ранг $\mathbf{A}$, а $(\mathbf{M}, \ \mathbf{b})$ является $n \times (3k+1)$-матрицей, получаемой присоединением вектора-столбца $\mathbf{b}$ к матрице $\mathbf{M}$. Следующая лемма полезна при изучении свойств неуязвимости линейных кодов.

Лемма 14.1. Пусть $\mathbf{M}$—$n \times l$-матрица; $\mathbf{b} = (b_1, \ b_2, \ \ldots, \ b_n)^T$ — вектор-столбец с элементами из $GF(q)$ и пусть $\mathbf{m}_i = (m_{i1}, m_{i2}, \ldots, m_{il})$, $i = 1, \ 2, \ \ldots, n$ обозначает i-ю строку $\mathbf{M}$. Тогда соотношение $\rho(\mathbf{M}) \neq \neq \rho(\mathbf{M}, \ \mathbf{b})$ выполняется тогда и только тогда, когда существует множество элементов $\{\alpha_i\}$ из $GF(q)$, таких, что $\sum_{i=1}^{n} \alpha_i \mathbf{m}_i = \mathbf{0}$ (где $\mathbf{0}$ — нулевой вектор), в то время как $\sum_{i=1}^{n} \alpha_i b_i \neq 0$.

Доказательство. Если $\rho(\mathbf{M}) = \rho$, то должны существовать ρ линейно независимых векторов $\mathbf{m}_j$, такие, что

$$\mathbf{m}_i = \sum_{j=1}^{\rho} \beta_j^{(i)} \mathbf{m}_j \text{ для всех } i. \tag{14.8}$$

Ясно, что соответствующее множество векторов $\{\mathbf{m}'_j\}$ из $(\mathbf{M}, \ \mathbf{b})$ также образует линейно независимое множество. Если также $\rho(\mathbf{M}, \ \mathbf{b}) = \rho$, то это множество $\{\mathbf{m}'_j\}$ должно порождать пространство $(\mathbf{M}, \ \mathbf{b})$ и

$$\mathbf{m}'_i = \sum_{j=1}^{\rho} \beta_j^{(i)} \mathbf{m}'_j \text{ для всех } i. \tag{14.9}$$

Для любого заданного i коэффициенты $\beta^{(i)}{}_j$ в ф-ле (14.8) определены однозначно. Если бы это было не так, то можно было бы указать линейную зависимость между векторами $\{\mathbf{m}_j\}$. Следовательно, так как первые l компонент $\mathbf{m}_i$ и $\mathbf{m}'_i$ совпадают, то то же самое справедливо для коэффициентов $\beta^{(i)}{}_j$ в ф-лах (14.8) и (14.9). Теперь

$$\sum_{i=1}^{n} \alpha_i \mathbf{m}_i = \sum_{j=1}^{\rho} \gamma_j \mathbf{m}_j. \tag{14.10}$$

где $\gamma_j = \sum_{i=1}^{n} \alpha_j \, \beta_j^{(i)}$ и

$$\sum_{i=1}^{n} \alpha_i \mathbf{m}'_i = \sum_{j=1}^{\rho} \gamma_j \mathbf{m}'_j. \tag{14.11}$$

Согласно предположению суммирование в ф-ле (14.10) дает нулевой вектор $\mathbf{0}$. Это означает, что $\gamma_j = 0$ для всех j, так как векторы $\{\mathbf{m}_j\}$ линейно независимы. В свою очередь, это означает, что сумма в (14.11) также равна $\mathbf{0}$, что противоречит предположению о том, что $\sum_i a_i b_i \neq 0$. Таким образом, если $\sum_i \alpha_i \mathbf{m}_i = \mathbf{0}$ и $\sum_i \alpha_i b_i \neq 0$, то для любого множества коэффициентов $\{\alpha_i\}$ имеем $\rho(\mathbf{M}, \mathbf{b}) > \rho(\mathbf{M})$. Обратно, если для любого множества $\{\alpha_i\}$, для которого $\sum_i \alpha_i \mathbf{m}_i = \mathbf{0}$, также $\sum_i a_i b_i = 0$, то, очевидно, $\rho(\mathbf{M}, \mathbf{b}) = \rho(\mathbf{M})$, и лемма доказана.

Следовательно, можно заключить, что словарь является неуязвимым при синхронизации на m-й позиции тогда и только тогда, когда условия представленной выше леммы удовлетворяются для некоторого множества элементов $\{\alpha_i\}$ и $\mathbf{M}$ и $\mathbf{b}$, определенных (14.6). Пусть $\{\alpha_i\}$ — множество элементов $GF(q)$, таких, что

$$\sum_i \alpha_i \mathbf{m}_i = \mathbf{0}. \tag{14.12}$$

Тогда, вспоминая определение матрицы $\mathbf{M}$ [см. (14.6)], находим, что должны выполняться следующие три равенства:

$$\left.\begin{aligned}
&\sum_{i=1}^{n} \alpha_i \mathbf{g}_i = \mathbf{0}.\\
&\sum_{i=n-m+1}^{n} \alpha_i \mathbf{g}_{i-(n-m)} = \sum_{i=1}^{m} \alpha_{i+n-m} \mathbf{g}_i = \mathbf{0};\\
&\sum_{i=1}^{n-m} \alpha_i \mathbf{g}_{i+m} = \sum_{i=m+1}^{n} \alpha_{i-m} \mathbf{g}_i = \mathbf{0},
\end{aligned}\right\} \tag{14.13}$$

где $\mathbf{g}_i$ представляет собой i-й столбец $\mathbf{G}$. Но по определению вектор $\mathbf{h} = (h_1, h_2, \ldots, h_n)$ принадлежит нуль-пространству кода, порождаемого $\mathbf{G}$, тогда и только тогда, когда

$$\sum_{i=1}^{n} h_i \mathbf{g}_i = \mathbf{0}. \tag{14.14}$$

Следовательно, (14.14) удовлетворяется на множестве $\{\alpha_i\}$ тогда и только тогда, когда нуль-пространство кода, порождаемого $\mathbf{G}$, содержит векторы $\mathbf{h} = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$; $\mathbf{h}^{(1)} = \{\alpha_{n-m+1}, \alpha_{n-m+2}, \ldots, \alpha_n, 0, 0, \ldots, 0\}$ и $\mathbf{h}^{(2)} = \{0, 0, \ldots, 0, \alpha_1, \alpha_2, \ldots, \alpha_{n-m}\}$. Этот вывод совместно с приведенной выше леммой доказывает следующую теорему.

Теорема 14.6. Если линейный (n, k)-код имеет смежный класс, который неуязвим при синхронизации на m-й позиции, то его нуль-пространство должно содержать три вектора: $\mathbf{h}=\{h_1, h_2, \ldots, h_n\}$; $\mathbf{h}^{(1)}=\{h_{n-m+1}, h_{n-m+2}, \ldots, h_n, 0, 0, \ldots, 0\}$ и $\mathbf{h}^{(2)}=\{0, 0, \ldots, 0, h_1, h_2, \ldots, h_{n-m}\}$, такие, что $\mathbf{h}\cdot\mathbf{c}\neq\mathbf{h}\cdot\mathbf{c}_m$, где $\mathbf{c}=\{c_1, c_2, \ldots, c_n\}$ — некоторый лидер смежного класса, а $\mathbf{c}^m \triangleq \{c_{m+1}, c_{m+2}, \ldots, c_n, c_1 \ldots, c_m\}$.

Таким образом, можно установить, может ли линейный код быть сделан неуязвимым при синхронизации на любой m-й позиции, определив, порождает ли его нуль-пространство три вектора, удовлетворяющие приведенным выше условиям. Это значительно облегчает определение возможного свойства такого кода быть кодом без запятой. Если код является циклическим, можно указать даже более простые необходимые и достаточные условия существования смежных классов без запятой. Их рассмотрение является предметом следующего параграфа.

14.4. Циклические коды без запятой

Если $\mathbf{G}$ порождает циклический (n, k)-код, то нуль-пространство кода также циклическое. Далее (см. § 13.4) нуль-пространство кода порождается $(n-k)\times n$-матрицей вида $\mathbf{H}=\{h_{ij}\}=\{h_{j-i+1}\}$ с $h_l=0$ для l, не принадлежащих интервалу $1\leqslant l\leqslant k+1$, но с неравными нулю h_1 и h_{k+1}. Это, совместно с результатами предыдущего параграфа, дает возможность доказать следующую теорему.

Теорема 14.7. Любой циклический (n, k)-код можно сделать неуязвимым при синхронизации на всех m позициях при $1\leqslant|m|\leqslant n-k-1$, $(|m| \triangleq \min(m, n-m))$ просто сложением некоторого ненулевого элемента кодового поля с первым символом каждого кодового слова.

Доказательство. Если $1\leqslant m\leqslant n-k-1$, то нуль-пространство кода содержит, очевидно, три вектора $\mathbf{h}=(h_1, h_2, \ldots, h_{k+1}, 0, 0, \ldots, 0)$; $\mathbf{h}^{(1)}= (0, 0, \ldots, 0)$ и $\mathbf{h}^{(2)}=(0, 0, \ldots, h_1, h_2, \ldots, h_{k+1}, 0, \ldots, 0)$. Так как $\mathbf{c}= (\alpha, 0, \ldots, 0)$ для некоторого $\alpha\neq0$, то

$$\mathbf{h}\cdot\mathbf{c}=h_1\alpha\neq\mathbf{h}\cdot\mathbf{c}^m=0, \tag{14.15}$$

если $1\leqslant m\leqslant n-k-1$, и условия теоремы 14.6 удовлетворяются. Точно такие же рассуждения приводят к тому же выводу для $1\leqslant n-m\leqslant n-k-1$. Следовательно, ур-ние (14.6) не будет иметь решений, когда $\mathbf{c}$ определяется таким образом при любых m, удовлетворяющих неравенствам $1\leqslant|m|\leqslant n-k-1$; теорема доказана.

Другие смежные классы, отличные от тех, которые образуются сложением элементов с первым столбцом, могут также обладать аналогичным свойством. Например, в равной мере эффективным будет сложение ненулевого элемента с каждым членом последнего столбца.

Справедлива также теорема, обратная теореме 14.7.

Теорема 14.8. Все смежные классы любого систематического (n, k)-кода уязвимы при синхронизации на всех m позициях, где $n-k \leqslant m \leqslant k$.

Доказательство. Первые k столбцов порождающей матрицы $\mathbf{G}$ любого систематического кода должны быть линейно независимыми. Если $n-k \leqslant m \leqslant k$, то никакое подмножество из первых $n-m \leqslant \leqslant k$ столбцов $\mathbf{G}$ и, следовательно, из первых $n-m$ строк $\mathbf{M}$ не может быть линейно зависимым. Но, кроме того, никакие из последних $m \leqslant k$ строк $\mathbf{M}$ не могут быть линейно зависимыми, так как столбцы $\mathbf{G}_1$ линейно независимы. Поэтому $\rho(\mathbf{M})=n$ и условия теоремы 14.6 не выполняются. ■

Следствие. Если $k \leqslant (n-1)/2$, то любой циклический (n, k)-код может быть превращен в код без запятой. Если $k > (n-1)/2$, то никакой смежный класс никакого циклического (n, k)-кода не образует код без запятой.

Доказательство следует из того, что все ошибочно синхронизируемые позиции могут быть сделаны неуязвимыми, когда $n-k-1 \geqslant k$, т. е. когда $k \leqslant (n-1)/2$. Так как все циклические коды являются систематическими кодами, то применима теорема 14.8, и если $k > (n-1)/2$, то все те величины m, которые лежат в интервале $(n-k, k)$, являются уязвимыми при синхронизации независимо от рассматриваемого смежного класса. ■

Возникает вопрос, имеют ли нециклические линейные коды, исправляющие ошибки, смежные классы без запятой и, в частности, существуют ли такие смежные классы при $k > (n-1)/2$. Интуитивно можно было бы предположить, что условия теоремы 14.6 выделяют циклические коды среди всех кодов с точки зрения свойства «свободы от запятой». Однако представляется трудным построить общее утверждение относительно этого свойства для смежных классов нелинейных циклических кодов, хотя частные коды или классы кодов иногда легко исследовать, используя указанные здесь методы.

Рассмотрим в качестве примера класс укороченных циклических $(n-\nu, k-\nu)$-кодов, получаемых отбрасыванием ν информационных битов из циклического (n, k)-кода (см. § 13.6). Нуль-пространство такого кода порождается матрицей $\mathbf{H}_\nu$, получающейся, когда отпускаются первые ν столбцов порождающей матрицы нуль-пространства первоначального циклического кода. Имея это в виду, нужно лишь повторить доказательство теоремы 14.7 (считая $\mathbf{h}$ $(\nu+1)$-й строкой $\mathbf{H}_\nu$) для того, чтобы доказать следующее.

Теорема 14.9. *Любой укороченный циклический $(n-\nu, k-\nu)$-код можно сделать неуязвимым при синхронизации на всех позициях m для $1 \leqslant |m| \leqslant n-k-\nu-1$, просто складывая некоторый ненулевой элемент с первым символом каждого кодового слова.*

Хотя теорема 14.8 применима также и к укороченным циклическим кодам, строгое обращение теоремы 14.9 оказывается в общем случае невозможным. Двоичный циклический (7, 3)-код мо-

15*

жет, например, быть сделан неуязвимым при синхронизации на m-й позиции для всех $1 \leqslant |m| \leqslant 3$ и поэтому превращен в код без запятой. Теорема 14.9 устанавливает существование укороченного циклического (6, 2)-кода, который неуязвим на позициях $1 \leqslant |m| \leqslant 2$, и (5,1)-кода, неуязвимого только на позициях $|m|=1$. Легко проверить, что ранг матрицы $\mathbf{M}$ (см. § 14.3), соответствующий укороченному циклическому (6, 2)-коду, равен 6, когда $m=3$, так что все его смежные классы являются, на самом деле, уязвимыми на позиции $m=3$, несмотря на то, что $k<(n-1)/2$. В противоположность этому укороченный циклический (5, 1)-код имеет смежный класс без запятой.

Рассмотрим второй пример класса нециклических кодов. Пусть $\mathbf{G}$ — $n \times k$-матрица, строки которой порождают слова циклического двоичного хэмминговского (n, k)-кода ($2^{n-k}=n+1$; см. § 13.6) и пусть $\mathbf{G}'$ получается из $\mathbf{G}$ некоторой перестановкой столбцов. Тогда $\mathbf{G}'$ также порождает двоичный (n, k)-код с теми же самыми расстояниями и поэтому с теми же самыми корректирующими свойствами, как и код, порождаемый $\mathbf{G}$. Все такие коды будут называться здесь кодами Хэмминга, хотя в общем случае они не будут циклическими. (Между прочим, можно проверить, что все двоичные линейные коды, исправляющие одну ошибку и имеющие $2^k=2^n/(n+1)$ слов, могут порождаться матрицей вида $\mathbf{G}'$.) Так как $k>(n-1)/2$ для всех таких кодов, кроме (3, 1)-кода, то никакой смежный класс никакого циклического хэмминговского кода не будет кодом без запятой при любых $k>1$. Возможно, однако, что некоторый смежный класс нециклического хэмминговского кода мог бы быть кодом без запятой даже при $k>1$.

Для того чтобы показать, что это невозможно, достаточно опять-таки доказать, что $\rho(\mathbf{M}')=n$ для некоторой уязвимой позиции m, где $\mathbf{M}'$ определяется через $\mathbf{G}'$ равенством (14.6). Каждая строка матрицы нуль-пространства двоичного хэмминговского кода содержит ровно $(n+1)/2$ *единиц* (см. § 13.6). Рассмотрим матрицу $\mathbf{M}'$, когда $m=(n-1)/2$. Так как в любое проверочное соотношение должны входить ровно $(n+1)/2$ столбцов $\mathbf{G}'$ и так как в этом случае $\mathbf{G}'_1$ содержит лишь $(n-1)/2$ столбцов, то никакое подмножество нижних $(n-1)/2$ строк $\mathbf{M}'$ не является линейно зависимым. Единственной остающейся возможностью является то, что линейно зависимыми окажутся верхние $(n+1)/2$ строк $\mathbf{M}'$. Легко заметить, что это означает, что

$$\sum_{i=1}^{(n+1)/2} \mathbf{g}_i' = \sum_{i=(n+1)/2}^{n} \mathbf{g}_i' = \mathbf{0},$$

где $\mathbf{g}'_i$ обозначает i-й столбец порождающей матрицы $\mathbf{G}'$. В свою очередь, отсюда следует, что $\sum\limits_{\substack{i=0 \\ i \neq (n+1)v2}}^{n} \mathbf{g}'_i=\mathbf{0}$, т. е. линейная комбинация $n-1$ столбцов $\mathbf{G}'$ должна быть равна нулю. Это противоречит условию, что ровно $(n+1)/2$ столбцов должны быть использованы в любом таком соотношении, если только не имеет места случай $n-1=(n+1)/2$, т. е. случай $n=3$. Следовательно, (3, 1)-код является единственным двоичным хэмминговским кодом со смежным классом без запятой.

Полезное видоизменение вида уравнения уязвимости (14.6) часто можно получить, представляя векторы, входящие в это уравнение, в виде многочленов, как в § 13.4. В этих обозначениях ф-ла (14.7) примет вид

$$w(x)+q_m(x)+x^{n-m}p_m(x)=c(x)(x^{n-m}-1),\ (\operatorname{mod} x^n-1), \tag{14.16}$$

где $w(x)=\sum\limits_{i=0}^{n-1} w_i x^i$ представляет собой некоторое слово $\mathbf{w}=(w_0, w_1, \ldots, w_{n-1})$ из словаря D, порожденного $\mathbf{G}$; $q_m(x)$ — многочлен степени, самое большее, $n-m-1$, соответствующий суффиксу из D, а $p_m(x)$ — многочлен степени, самое большее, $m-1$, соответствующий префиксу из D. Многочлен $c(x)$ соответствует лидеру смежного класса. (Заметим, что здесь термин «лидер смежного класса» обозначает любой элемент в смежном классе, а не обязательно элемент минимального веса.)

Если код является циклическим, то $p_m(x)$ является также суффиксом, а $q_m(x)$ — префиксом из D. Если это так, то уравнение уязвимости можно выразить более просто в одном из двух видов $w(x)=c(x)(x^{n-m}-1)-x^{n-m}p_m(x)$ или

$$w(x)=c(x)(x^{n-m}-1)-q_m(x). \tag{14.17}$$

При этом словарь является уязвимым при синхронизации на позиции m тогда и только тогда, когда правая часть (14.17) является кодовым словом. Вспомнив, что согласно § 13.4 многочлен $p(x)$ представляет собой слово циклического кодового словаря D, порождаемого многочленом $g(x)$, тогда и только тогда, когда синдром $\{p(x)\}\triangleq r(x)$ тождественно равен нулю [где $p(x)=q(x)g(x)+r(x)$] получаем условия неуязвимости на m-й позиции $\{c(x)(x^{n-m}-1)-x^{n-m}p_m(x)\}\neq 0$ или

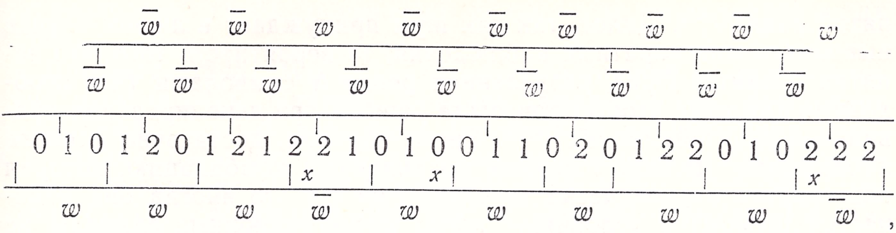
$$\{c(x)(x^{n-m}-1)-q_m(x)\}\neq 0. \tag{14.18}$$

Используя этот подход, можно очень просто доказать теоремы 14.7 и 14.8 (для циклических кодов). Во-первых, если $c(x)=1$ и если $m\leqslant n-k-1$, то $\{x^{n-m}-1-x^{n-m}p_m(x)\}=\{x^{n-m}[1-x^m-p_m(x)]\}\neq 0$, так как $p_m(x)$ имеет степень, самое большее, $m-1$, а $g(x)$ имеет степень $n-k$. Аналогично, если $1\leqslant n-m\leqslant n-k-1$, то $\{x^{n-m}-1-q_m(x)\}\neq 0$. Во-вторых, для того чтобы доказать теорему 14.8 для циклических кодов, нужно лишь заметить, что $\{c(x)(x^{n-m}-1)-x^{n-m}p_m(x)\}$ является многочленом степени, самое большее, $n-k-1$. Так как $p_n(x)$ представляет собой префикс из D, то его первые k коэффициентов соответствуют информационным символам и, следовательно, могут быть произвольны. Если $n-k\leqslant m\leqslant k$, то должен существовать многочлен $p_m(x)$, такой, что $\{x^{n-m}[c(x)(1-x^m)-p_m(x)]\}=0$ независимо от многочлена $c(x)$.

14.5. Синхронизация в каналах с шумами

Когда шума нет, синхронизация слов обычно устанавливается, если она может быть установлена вообще, с абсолютной надежностью. Как только появляется синхронизационная комбинация или как только устраняются все возможные декодирования последовательности (в силу того, что они приводят в некотором месте к последовательности, которая не является словом), кроме одного, синхронизация будет достигнута. Наличие шума может видоизменить задачу синхронизации в нескольких направлениях. Если, например, синхронизация должна устанавливаться опознанием некоторой специальной m-последовательности и кодовый словарь был тщательно выбран с тем, чтобы запретить появление этой m-последовательности в каком-либо неожиданном месте, шум может вызвать ложную синхронизацию, так изменив m-последовательность, появляющуюся внутри последовательности слов, что она будет воспринята приемником как синхронизационная комбинация. Более того, шум может увеличить синхронизационную задержку, изменив синхронизационную комбинацию и приводя к тому, что она пройдет незамеченной. Аналогично если синхронизация слов основывается на том, что ошибочно декодируемые последовательности с длинами, превосходящими некоторую конечную длину, не существуют, шум может аннулировать это свойство. Недекодируемая последовательность может перейти в декодируемую последовательность из-за наличия шума, в то время как первоначально декодируемая последовательность может стать недекодируемой.

Возможность ошибочной синхронизации в присутствии шума даже для синхронизируемых кодовых словарей неизбежно изменяет процедуру синхронизации. Теперь нужно выносить статистическое решение. Должна быть выбрана «наиболее близкая» декодируемая последовательность или комбинация, наибольшим образом напоминающая синхронизационную комбинацию, с последующим повторением процедуры через правильные интервалы. Если, например, используются коды без запятой с длиной слова n, то синхронизация устанавливается с помощью наблюдения всех принимаемых n-последовательностей для определения, являются они словами или нет. Так как в отсутствие шума никакой стык слов не является кодовым словом, то наиболее вероятно даже в присутствии шума, что правильные слова будут опознаваться как кодовые слова, а стыки — нет. И так как правильные кодовые слова должны наблюдаться после приема каждых n символов, то можно увеличить надежность синхронизационной оценки с помощью последовательного опознавания кодовых слов, разделенных ровно n символами. В качестве примера предположим, что слова из словаря без запятой $D=\{010, 011, 020, 021, 022, 120, 121, 122\}$ передаются по каналу с шумом и принимается последовательность:



где символы, обозначенные *x*, ошибочны. Так как при декодировании, которое представлено нижней разбивкой, сталкиваются лишь с двумя «не словами» (**w**), в то время как в двух других случаях почти все время сталкиваются с «не словами», то, по-видимому, нижняя разбивка соответствует правильной синхронизации. Те же соображения применимы к другим методам синхронизации, рассмотренным в предыдущих главах.

Это изменение в поисковой процедуре синхронизации, обусловленное присутствием шума, может изменить относительную привлекательность различных ограничений, наложенных на блоковые коды с целью сделать их синхронизируемыми. Два варианта синхронизационных ограничений из гл. 12, имеющие смысл, когда в канале связи действует шум, рассматриваются в нескольких следующих параграфах.

14.6. Последовательности Баркера

Первый вариант предусматривает ослабление одного из ограничений гл. 12. Код с запятой подчинялся ограничению, которое предотвращало появление некоторой специальной m-последовательности в любой произвольной последовательности слов из этого словаря. Когда бы эта m-последовательность или запятая не наблюдалась приемником, она была установлена преднамеренно и поэтому давала требуемую синхронизацию. Как уже было отмечено, в присутствии шума ситуация не является столь простой. По-видимому, необходимы многократные наблюдения запятой, чтобы увеличить вероятность того, что, на самом деле, была именно принята она и что это не был просто шумовой эффект. Один очевидный и простой метод синхронизации слов, который часто применяется, когда все равно приходится выполнять несколько наблюдений, состоит в периодической передаче запятой, как и раньше, но с отказом от каких-либо ограничений на остающуюся передаваемую последовательность.

Предположим, что в качестве запятой используется m-последовательность и она передается после каждых $N—m$ информационных символов. Запятая может теперь появиться в информационной последовательности даже в отсутствие шума. Но если информация представляет собой случайную последовательность r-ичных символов, выбираемых независимо и равновероятно, то вероятность любой заданной информационной m-последовательности быть запятой равна r^{-m}. Далее, так как шум принуждает в любом случае выполнять многократные наблюдения, то вероятность того, что запятая появится l раз, разделенная ровно N символами (что необходимо для того, чтобы произошла ошибка при декодировании правильной запятой), равна r^{-lm}. Таким образом, достаточно длинное наблюдение должно опознать правильную комбинацию, которая повторяется периодически (несмотря на то, что иногда она изменяется шумом) в условиях, когда информационные символы не подвергаются ограничению. Фактически возможное уменьшение времени, необходимого для вынесения надежного решения, которое достигается благодаря дополнительному ограничению на информационную последовательность, часто бывает незначительным.

С первого взгляда можно было бы предположить, что любая запятая была бы столь же хорошей, как и любая другая, так как все последовательности заданной длины появляются случайно с одной и той же вероятностью. Это было бы, по существу, верно, если бы не было также необходимости проводить различие между запятой и теми m-последовательностями, которые начинаются каким-либо из ее $m-1$ суффиксов или оканчиваются каким-либо из ее $m-1$ префиксов. Выбор запятой, состоящей из m повторений одного и того же символа, например, был бы, очевидно, плохим. Если бы такой запятой предшествовал или бы за ней следовал тот же самый символ, то, по меньшей мере, две подряд идущие m-последовательности были бы идентифицированы как запятые.

Пусть d_i — хэмминговское расстояние между i-символьным суффиксом запятой и ее i-символьным префиксом. Среднее расстояние запятой от m-последовательности, начинающейся ее i-символьным суффиксом и оканчивающейся $m-i$ независимыми r-ичными информационными символами, в отсутствие ошибок равно

$$d_i + \frac{r-1}{r}(m-i) = \frac{r-1}{r}\left[m - \left(i - \frac{r}{r-1}d_i\right)\right]. \qquad (14.19)$$

(Эта величина равна также расстоянию запятой от m-последовательности, начинающейся $m-i$ информационными символами и оканчивающейся i-символьным префиксом запятой.) Имея в виду сделанные замечания, подходящей запятой могла бы быть некоторая m-последовательность, для которой расстояния (14.19) максимальны для всех i. Это означает выбор последовательности, для которой величина

$$c_i \triangleq i - \frac{r}{r-1}d_i \qquad (14.20)$$

достигает минимально возможного значения для всех i, $0<i<m$.

Граница, определяемая следующей теоремой, будет полезна в дальнейшем.

Теорема 14.10. Пусть c_i определяются согласно (14.20). Тогда для любой r-ичной m-символьной запятой

$$\max_{1\leqslant i\leqslant m-1} c_i \geqslant \operatorname*{ave}_{1\leqslant i\leqslant m-1} c_i \geqslant \frac{m}{2} - \frac{r}{2(r-1)(m-1)}\left[m^2\left(\frac{r-1}{r}\right)\right],$$

где квадратные скобки обозначают целую часть заключенной в них дроби.

Доказательство. Пусть D — словарь, состоящий из m циклических перестановок запятой. Среднее хэмминговское расстояние d_{AVE} между запятой и ее $m-1$ различными циклическими перестановками, очевидно, равно среднему расстоянию между любыми двумя словами из D. Это расстояние ограничено границей Плоткина (13.11) следующим образом: $d_{\text{AVE}} \leqslant m^2(r-1)/(m-1)r$. Теперь из (14.20) имеем

$$\sum_{i=1}^{m-1} c_i = \frac{m(m-1)}{1} - \frac{r(m-1)}{2(r-1)} d_{\text{ave}}. \tag{14.21}$$

В силу того что $(m-1)_{\text{ave}}$ должно быть целым, отсюда непосредственно следует утверждение теоремы. ■

Первые исследования в этой области были выполнены Баркером и ограничивались последовательностями из двоичного алфавита. При первоначально наложенных ограничениях последовательности считались приемлемыми, только если $\max c_i \leqslant 0$. Рассмотрим вначале следствия этого условия.

Теорема 14.11. Если существует двоичная последовательность длины m с $c_i \leqslant 0$ для всех i, $i=1, 2, \ldots, m-1$, то

$$c_i = \begin{cases} 0, & i \text{ четное;} \\ -1, & i \text{ нечетное.} \end{cases}$$

Более того, такие последовательности могут существовать с длиной $m>2$, только если $m=4t-1$ для некоторого целого t.

Доказательство. Если $r=2$, то величина $c_i = i - 2d_i$ должна быть четным целым числом при четном i и нечетным целым числом при нечетном i. Предположим, что $\gamma_1\gamma_2\ldots\gamma_m$ — последовательность, для которой

$$c_i = \begin{cases} -1, & i \text{ нечетное;} \\ 0, & i \text{ четное.} \end{cases}$$

Тогда $$\sum_{i=1}^{m-1} c_i = -\left[\frac{m}{2}\right],$$

и эта сумма находится на границе из теоремы 14.10. Любая последовательность $\gamma'_1\gamma'_2\ldots\gamma'_m$, имеющая некоторые параметры $c'_i < c_i$, обязательно имеет, по меньшей мере, один член c'_j, больший, чем соответствующее c_j. Это означает, что $c'_j \geqslant c_j + 2 \geqslant 1$ и, следовательно, нарушается условие $\max c_i \leqslant 0$.

Чтобы доказать второе утверждение теоремы, отметим, что для любой двоичной последовательности $\gamma_1\gamma_2\ldots\gamma_m$ справедливо равенство

$$a_i \triangleq c_i + c_{m-i} = \sum_{\nu=1}^{m} (1-2\gamma_\nu)(1-2\gamma_{\nu+i}) =$$

$$= m - 4\sum_{\nu=1}^{m}\gamma_\nu + 4\sum_{\nu=1}^{m}\gamma_\nu\,\gamma_{\nu+i} = m - 4\,l \tag{14.22}$$

для некоторого целого l. (Подстрочные индексы у γ_i понимаются по модулю m.) Но, как мы только что показали, когда m четное и $\max c_i \leqslant 0$,

$$a_i = c_i + c_{m-i} = \begin{cases} 0, & i \text{ четное;} \\ -2, & i \text{ нечетное.} \end{cases}$$

При этом нарушается условие (14.22) (кроме случая $m=2$) так, что m не может быть четным целым числом, большим, чем 2. Если m нечетное, то $a_i = -1$ для всех $i \neq 0$ по модулю m и из ф-лы (14.22) $m = 4l - 1$, что и требовалось показать. ■

Баркер смог построить последовательности с требуемым свойством (при $m>2$) для длин $m=3$, 7 и 11 и предположил, что не существует никаких других таких последовательностей. (Если $m=1$, то, очевидно, требуемым условием удовлетворяет тривиальная последовательность 1, а если $m=2$, то такой последовательностью является последовательность 10.) Впоследствии было доказано, что это предположение верно. Последовательности, найденные Баркером, были следующими:

$m=3$ 110
$m=7$ 1110010
$m=11$ 11100010010.

(Эквивалентные последовательности получаются при обращении этих последовательностей и замене либо четных, либо нечетных символов на дополнительные. Баркер, между прочим, заметил, что при построении этих последовательностей полезно знать, что всегда должны удовлетворяться соотношения $\gamma_i \neq \gamma_{m+1-i}$ для нечетных i и $\gamma_i = \gamma_{m+1-i}$ для четных i. Это легко доказать методом индукции по i.)

В силу того что при первоначальных баркеровских ограничениях существуют только три неэквивалентные последовательности, то были предприняты попытки найти другие последовательности при несколько более слабых ограничениях. Первым очевидным ослаблением ограничения на коэффициенты c_i является разрешение иметь $c_i = 1$ для некоторых значений i. Более того, так как, по-видимому, нет преимуществ от того, что величины c_i будут принимать большие отрицательные значения (ср. с теоремой 14.11) а, наоборот, это может иногда принести вред, то сразу же возникает условие $|c_i| \leqslant 1$, $0 < i < m$. Двоичные последовательности, удовлетворяющие этому условию, обычно называются *последовательностями Баркера;* они найдены для длин $m=1$, 2, 3, 4, 5, 7, 11 и 13. Было показано, что такие последовательности не существуют для нечетных длин $m>13$. (Тем самым, конечно, доказывается несуществование каких-либо последовательностей, удовлетворяющих первоначальному условию Баркера, для любых длин $m>11$).

Теорема 14.12. Пусть $\gamma_1\gamma_2\ldots\gamma_m$ — двоичная последовательность с коэффициентами c_i, ограниченными по абсолютной величине единицей для всех $i=1, 2, \ldots, m-1$. Тогда, если m четное целое число, большее 2, то $m=4v^2$, где v — целое. Если m нечетное, то $c_i = (-1)^{(m-1)/2}$, когда i нечетное и $c_i=0$, когда i четное, $0<i<m$.

Доказательство. Если $|c_i|\leqslant 1$, то $|c_i|=1$ для всех нечетных i и $c_i=0$ для всех четных i. Таким образом, когда m четное,

$$a_i = c_i + c_{m-i} = \begin{cases} 0 & , \quad i \text{ четное}, \ i \neq 0; \\ 0, \ +2 \text{ или } -2, & i \text{ нечетное}. \end{cases}$$

Но из (14.6.4) следует, что $a_i - a_j = 4l$ для некоторого целого l и для всех целых i, j. Аналогично если m четное и больше 2, то $a_i=0$ для всех $i=1, 2, \ldots, m-1$. Полагая $\alpha_1 = 1-2\gamma_i$, находим

$$\sum_{i=1}^{m} a_i = m = \sum_{i=1}^{m}\sum_{j=1}^{m} \alpha_j \alpha_{j+i} = \left(\sum_{j=1}^{m} \alpha_j\right)^2 = t^2 \tag{14.23}$$

для некоторого целого i. Так как m четное, то t должно быть четным и $m=(2v)^2$ для некоторого целого v. Если m нечетное и $|c_i|\leqslant 1$, то $a_i = (-1)^{(m-1)/2}$ [ср. с (14.22)]. Таким образом, так как c_i четны, когда i четное, и нечетны в противном случае, то $c_i = (-1)^{(m-1)/2}$, когда i нечетное, и $c_i=0$, когда i четное. ■

Не существуют баркеровские последовательности четной длины при всех v из отрезка от 2 до 54 ($16\leqslant m\leqslant 11\,664$)[1]. Существование каких-либо баркеровских последовательностей с длинами, отличными от приведенных выше, кажется крайне невероятным.

Дальнейшее обобщение основывается на замечании, что для больших значений m полезно ослабить далее ограничения на $|c_i|$. Представляется, что довольно трудно получить теоретические результаты, когда $|c_i|$ не ограничены единицей. Последовательности, для которых $|c_i|\leqslant 2$, были найдены для всех длин $m\leqslant 21$ и для $m=25$ и 28; в случае, когда накладывается ограничение $|c_i|\leqslant 3$, известны последовательности для всех длин $m\leqslant 34$.

Очевидно, что коэффициент c_i не может быть равномерно малым, если это свойство не выполняется для $a_i = c_i + c_{m-i}$. Обратное этому утверждение, что c_i будут равномерно малыми, если малы a_i, конечно, не обязательно верно. Тем не менее поиск последовательности баркеровского типа можно было бы начать с последовательностей, про которые известно, что они имеют малые значения a_i, например, с последовательностей регистра сдвига максимальной длины (см. теорему 13.11). В силу того что коэффициенты c_i различны для различных циклических перестановок последовательности, каждая последовательность максимальной длины с длиной m может порождать вплоть до m неэквивалентных синхронизирующих последовательностей. В качестве примера рассмотрим последовательность $S_0 = 1110100$ и определим S_i как последовательность S_0, циклически сдвинутую на i позиций вправо. Коэффициенты c_i для этих семи последовательностей приведены в табл. 14.1. Хотя все эти последовательности ведут себя достаточно хорошо с точки зрения максимального значения коэффициента c_i, но лишь одна из них $S_4=0100111$ является баркеровской последовательностью:

---

[1] Последовательность 1110 и все ее перестановки являются баркеровскими последовательностями длины 4. *(Прим. авт.)*.

Таблица 14.1

c_i	S_0	S_1	S_2	S_3	S_4	S_5	S_6
c_6	0	—2	0	0	0	—2	—2
c_5	1	1	—1	—3	—1	—1	—1
c_4	0	—2	—2	—2	0	0	2
c_3	—1	1	1	1	—1	—1	—3
c_2	—2	—2	0	2	0	0	0
c_1	—1	1	—1	—1	—1	1	1

Очень мало известно о последовательностях баркеровского типа в недвоичном случае. Однако снова множество последовательностей регистра сдвига максимальной длины (когда r — простое число или степень простого числа) представляется подходящим множеством для поиска в нем последовательностей баркеровского типа. Среднее значение коэффициентов c_i, связанных с этими последовательностями, как легко проверить, по крайней мере, достигает нижней границы, данной в теореме 14.10.

14.7. Индекс свободы от запятой

Другой метод получения синхронизации слов в присутствии шума состоит опять-таки в кодировании информации, но при ограничении, более жестком, чем обычная свобода от запятой. Условие свободы от запятой гарантирует, что каждый стык слов отличается от каждого кодового слова, по меньшей мере, в одном символе. Шум с большой вероятностью может устранить это различие и привести к удлинению времени синхронизационного поиска. Однако если каждый стык слов отличается от каждого кодового слова, по крайней мере, $s>1$ символами, то вероятность того, что шум нейтрализует это различие, должна соответственно понизиться. Следовательно, кодовые слова могли бы легче отличаться от стыка слов, что привело бы к увеличению быстроты установления синхронизации слов и ее надежности. Коды, которые удовлетворяют требованию, что каждый стык слов отличается от каждого кодового слова, по меньшей мере, в s позициях, будут называться *кодами без запятой с индексом* s[1]).

---

[1]) Используется также термин «код с разделением s». (*Прим. отв. ред.*).

Некоторые из методов построения кодов без запятой (гл. 12) можно обобщить для того, чтобы получить коды с большими индексами свободы от запятой. Однако в дальнейшем не будем следовать этому подходу в силу того, что возникают довольно серьезные ограничения при практическом использовании таких кодов, например, недостаточная защищенность против ошибок после установления синхронизации. Два кодовых слова в коде без запятой с большим индексом могут различаться лишь одним символом. Предполагается, что шум относительно легко трансформирует один символ в другой, иначе не было бы необходимости использовать большой индекс свободы от запятой. При этих условиях будет происходить много ошибочных декодирований. В то время как потеря синхронизации может быть исправлена с помощью дальнейших наблюдений, ошибочно декодированное кодовое слово обычно не повторяется второй раз. Следовательно, разумно потребовать чтобы минимальное расстояние между кодовыми словами было бы, по меньшей мере, таким же, как минимальное расстояние между кодовыми словами и стыками. В общем случае мы будем интересоваться словарями, для которых первое расстояние значительно больше, чем второе.

Довольно простую границу для числа кодовых слов в таких словарях может дать следующее утверждение.

Теорема 14.13. Если r-ичный словарь D, содержащий N n-символьных слов, имеет индекс свободы от запятой s и минимальное расстояние, по меньшей мере, равное s, то

$$N \leqslant N_s(n, r) = W_s(n, r)/n, \tag{14.24}$$

где $W_s(n, r)$ — максимальное число n-символьных r-ичных слов в словаре (не обязательно линейном), имеющем минимальное хэмминговское расстояние s.

Доказательство. Каждая циклическая перестановка каждого кодового слова не должна совпадать с каждой циклической перестановкой каждого другого слова и с каждой другой циклической перестановкой самого себя, по меньшей мере, в s символах, если код является кодом без запятой с индексом s и одновременно обладает минимальным расстоянием s. Словарь, содержащий все n циклических перестановок каждого кодового слова из D, имеет тогда nN кодовых слов, которые должны быть разделены минимальным хэмминговским расстоянием s. Не может быть более чем $W_s(n, r)$ таких слов. ■

Заметим, что, когда $s=1$, получаем границу $N \leqslant r^n/n$, которая, конечно, справедлива, но не является минимальной границей для числа слов в обычных кодовых словарях без запятой.

Следствие. Словарь, содержащий N n-символьных r-ичных слов, не может иметь индекс свободы от запятой, больший, чем

$$s \leqslant \min_{\rho_0 \leqslant \rho \leqslant [(r-1)/r]n} \left\{ \frac{N_\rho}{N_\rho - 1} \rho \left(2 - \frac{\rho}{n} \frac{r}{r-1}\right), 2\rho \right\}, \tag{14.25}$$

где N_ρ — наименьшее целое число больше или равное $(nN/r^n)\times$ $\times\sum_{i=0}^{\rho}\binom{n}{i}(r-1)$, а ρ_0 — наименьшее целое, такое, что $N_{\rho_0}\geqslant 2$.

Доказательство. Это утверждение следует немедленно, если использовать границу теоремы 13.2 для $W_s(n, r)$ в теореме 14.13. ■

В некоторых случаях может оказаться более важным обнаруживать потерю синхронизации, а не определять ее вначале непосредственно по последовательности кодовых слов. Эта ситуация может возникнуть, например, тогда, когда режим входа в синхронизм предшествует режиму передачи (что дает возможность установить необходимую начальную синхронизацию), но когда вероятностью последующей потери синхронизма нельзя пренебречь. Потеря синхронизма часто возникает из-за того, что местный сигнал отсчета слов сдвинулся на несколько символьных позиций от правильной позиции.

Поэтому полезно определить *индекс неуязвимости* s_m, указывающий, что любой стык, начинающийся $(m+1)$-м символом одного слова и кончающийся m-м символом второго слова, должен отличаться, по меньшей мере, s_m символами от любого правильного кодового слова. Ранее указывалось на некоторые преимущества использования словаря с большим индексом неуязвимости на всех позициях m из некоторого отрезка $-\mu\leqslant m\leqslant\mu$ за счет, возможно, полного отсутствия неуязвимости для других значений m. Будем характеризовать с помощью *индекса неуязвимости s степени μ* любой словарь с индексом неуязвимости, по меньшей мере, равным s на всех позициях m, $1\leqslant|m|\leqslant\mu$. Очевидно, что если $\mu=[n/2]$, где n — длина кодового слова, то словарь является словарем без запятой с индексом s. Границу теоремы 14.13 можно легко обобщить так, чтобы охватить коды с индексами неуязвимости произвольной степени.

Теорема 14.13а. Если r-ичный словарь D, содержащий N n-символьных слов, имеет индекс неуязвимости s степени $\mu\leqslant n-1$ и минимальное расстояние, по меньшей мере, s, то $N\leqslant$ $\leqslant W_s(n, r)/(\mu+1)$, где $W_s(n, r)$ было определено ранее [см. (14.24)].

Доказательство. Пусть $\mathbf{w}$ — слово из D, а $\mathbf{w}^m$ — n-последовательность, получаемая при циклическом сдвиге символов $\mathbf{w}$ на m позиций вправо. Пусть S — множество всех n-последовательностей $\mathbf{w}^m$, где $\mathbf{w}$ — любое слово из D, а m — любое целое число из отрезка $-[\mu/2]\leqslant m\leqslant[(\mu+1)/2]$. Если любые две из этих n-последовательностей, скажем, $\mathbf{w}_1^{m_1}$ и $\mathbf{w}_2^{m_2}$ находятся на расстоянии σ одна от другой, то кодовое слово $\mathbf{w}_1$ находится на расстоянии σ от сдвинутого кодового слова $\mathbf{w}^{m_2-m_1}$. Так как по построению $|m_2-m_1|\leqslant$ $\leqslant\mu$, то $(\mu+1)N$ n-последовательностей из S должны быть отделены друг от друга расстоянием, по меньшей мере, равным s, и теорема доказана.

14.8. Вычисление индекса неуязвимости смежных классов линейных кодов

Используя обозначения §14.3, напомним, что смежный класс линейного кода, порождаемого столбцами матрицы $\mathbf{G}$, является уязвимым при синхронизации на m-позиции тогда и только тогда, когда уравнение

$$\mathbf{M}\mathbf{v}=\mathbf{b} \tag{14.26}$$

имеет решение, т. е. тогда и только тогда, когда

$$\rho\mathbf{M}=\rho(\mathbf{M},\ \mathbf{b}) \tag{14.27}$$

где $\mathbf{M}$ и $\mathbf{b}$ определены в ф-ле (14.6). Предположим теперь, что для некоторого значения m и некоторого вектора $\mathbf{v}$

$$\mathbf{M}\mathbf{v}-\mathbf{b}=\mathbf{e}(\mathbf{v},\ m). \tag{14.28}$$

Предположим далее, что матрица $\mathbf{G}$ такова, что

$$\min_{\substack{\mathbf{v},\ m\\ 1\leqslant m\leqslant\mu}} |\mathbf{e}(\mathbf{v},\ m)|=|\mathbf{e}(\mathbf{v}_0,\ m_0)|=|\mathbf{e}|=s, \tag{14.29}$$

где $|\mathbf{e}(\mathbf{v},\ m)|$ обозначает хэмминговский вес $\mathbf{e}(\mathbf{v},\ m)$. Смежный класс, получающийся при сложении $\mathbf{c}$ со словарем, порождаемым $\mathbf{G}$, имеет тогда индекс неуязвимости s степени μ. В этом случае

$$\rho(\mathbf{M})=\rho(\mathbf{M},\ \mathbf{b}+\mathbf{e}) \tag{14.30}$$

для $m=m_0$, но это равенство не справедливо для любого $\mathbf{e}$ меньшего веса при любом m из отрезка $1\leqslant|m|\leqslant\mu$.

К сожалению, не существует достаточно удобного метода определения минимального значения $|\mathbf{e}|$ в случае, когда оно не равно нулю. Следующий метод полезен, когда хотят получить верхнюю границу для $|\mathbf{e}|$ при заданной матрице $\mathbf{G}$, когда хотят найти $|\mathbf{e}|$ для заданного смежного класса, и в некоторых случаях для построения оптимального лидера смежного класса для заданной порождающей матрицы $\mathbf{G}$. Однако с ростом длины кода необходимые вычисления становятся весьма громоздкими, и первая из этих задач является, по-видимому, единственной, для которой этот метод является полезным при любых, но относительно малых кодовых словарях.

Процедура состоит в следующем. Определяется операторная матрица $\mathbf{A}$, которая приводит $\mathbf{M}$ к приведенно-ступенчатой канонической форме

$$\mathbf{A}\,\mathbf{M}=\begin{pmatrix}\mathbf{B}\\ \mathbf{0}\end{pmatrix}, \tag{14.31}$$

где $\mathbf{B}$ — $\rho_0\times3k$-матрица; ρ_0 — ранг $\mathbf{M}$, а $\mathbf{0}$ — нулевая матрица. Умножая обе части (14.28) на $\mathbf{A}$, получаем

$$\mathbf{A}\mathbf{M}\mathbf{v}=\mathbf{A}\mathbf{b}+\mathbf{A}\mathbf{e} \tag{14.32}$$

В силу того что $\rho(\mathbf{M})=\rho_0$, первые ρ_0 написанных выше уравнений могут быть разрешены. Левые части каждого из остающихся $n-\rho_0$ уравнений равны всегда нулю, поэтому $\mathbf{e}$ должно выбираться так, чтобы удовлетворялось уравнение

$$\widetilde{\mathbf{A}\mathbf{b}} = -\widetilde{\mathbf{A}\mathbf{e}}, \tag{14.33}$$

где тильда обозначает усеченные векторы, состоящие лишь из $n-\rho_0$ последних компонент. Имеются q^n способов выбора $\mathbf{e}$ над $GF(q)$, но имеются лишь $q^{n-\rho_0}$ векторов $\widetilde{\mathbf{A}\mathbf{e}}$. Можно систематически перебирать все эти векторы, начиная с вектора $\mathbf{e}$ наименьшего веса и переходя к векторам все большего веса до тех пор, пока все $q^{n-\rho_0}$ векторов из множества $\widetilde{\mathbf{A}\mathbf{e}}$ не будут представлены хотя бы один раз. Вес s вектора максимальной длины, который завершает множество, дает границу для индекса неуязвимости словаря на позиции m. Этот индекс можно реализовать, если существует вектор $\mathbf{c}$, удовлетворяющий (14.33). Если для каждого другого значения m из отрезка $1 \leqslant |m| \leqslant \mu$ $\mathbf{c}$ также приводит к вектору $\mathbf{e}$ веса, по меньшей мере равного s, то словарь имеет индекс неуязвимости s степени μ.

Из ур-ния (14.32) следует, между прочим, другая довольно полезная граница для индекса неуязвимости, достижимая на линейных кодах.

Теорема 14.14. Индекс неуязвимости s_m на позиции m любого смежного класса линейного кода, порожденного $\mathbf{G}$, не может превосходить $n-\rho_0$, где $\rho_0 = \rho(\mathbf{M})$ — ранг матрицы $\mathbf{M}$ из (14.26).

Доказательство. Для того чтобы привести $\mathbf{M}$ к приведенно-ступенчатой канонической форме, необходимо лишь выбрать ρ_0 линейно независимых строк $\mathbf{M}$, сложить эти строки, умноженные на подходящие коэффициенты, с каждой из остальных и с оставшимися строками $\mathbf{M}$ и, наконец, переставить строки полученной матрицы. Если $\mathbf{A}$ — матрица, выполняющая эти операции, а $\mathbf{e}$ — вектор с нулями на ρ_0 позициях, соответствующих этим линейно независимым строкам $\mathbf{M}$ и с произвольными компонентами на остальных позициях, то $\mathbf{A}\mathbf{e}$ представляет собой просто перестановку $\mathbf{e}$, при которой ненулевые компоненты $\mathbf{e}$ переставлены на $n-\rho_0$ последних позиций. Так как эти компоненты произвольны, то равенство (14.33) всегда можно удовлетворить вектором $\mathbf{e}$ веса, не большего $n-\rho_0$. ■

Следствие. Индекс неуязвимости систематического (n, k)-кода на любой позиции m

$$s_m \leqslant \begin{cases} n-|m|-k, & |m| \leqslant k, \quad n-k; \\ n-2k, & |m| > k, \end{cases} \tag{14.34}$$

где $|m| \triangleq \min(m, n-m)$.

Доказательство. Если матрица $\mathbf{G}$ порождает систематический код, то первые ее k столбцов линейно независимы. Предположим, что $m \leqslant n/2$. Тогда первые m столбцов $\mathbf{G}_1$ в (14.6), если $m \leqslant k$ и $m \leqslant n-k$, или первые k столбцов, если $k < m < n-k$, также являются линейно независимыми. Матрица $\mathbf{M}$ должна поэтому содержать, по меньшей мере, $k+m$ и $2k$ линейно независимых строк соответственно этим двум случаям, и ранг ρ_0 матрицы $\mathbf{M}$ соответствующим образом ограничен снизу. Если m заменяется на $|m|$, то та же самая граница, очевидно, справедлива при $m>n/2$. Так как $s_m \leqslant n-\rho_0$ (теорема 14.4), то следствие доказано.

14.9. Индекс неуязвимости циклических кодов

Как было доказано в § 14.4, смежный класс циклического кодового словаря D является неуязвимым при синхронизации на m-й позиции, кроме случая, когда многочлен

$$c(x)(x^{n-m}-1)-x^{n-m}p_m(x) \tag{14.35}$$

либо, что эквивалентно, многочлен $c(x)(x^{n-m}-1) - q_m(x)$ представляет собой кодовое слово из D по модулю многочлена x^n-1. Многочлен $c(x)$ соответствует лидеру смежного класса, а $p_m(x)$ и $q_m(x)$ — многочлены степеней, не больших $m-1$ и $n-m-1$ соответственно. Обобщая это доказательство, заключаем, что минимальное число коэффициентов любого многочлена из (14.35), которые должны быть изменены так, чтобы получился многочлен кодового слова, равно индексу неуязвимости s_m на позиции m данного рассматриваемого смежного класса. Заметим, между прочим, что для любого смежного класса любого циклического кода $s_{n-m}= =s_m$. Это следует из того, что если s_m соответствующих коэффициентов многочленов $c(x)(x^{n-m}-1)-x^{n-m}p_m(x)$ и $w(x)$ отличаются друг от друга, то же самое справедливо для s_m коэффициентов многочленов $c(x)(1-x^m)-p_m(x)$ и $x^m w(x)=w'(x)$. Но, если $w(x)$ представляет собой слово циклического кода (а не смежного класса), то $w'(x)$ — тоже кодовое слово, а если $p_m(x)$ является префиксом из этого кода, то он также должен быть и суффиксом.

Теорема 14.15. Пусть D_0 и D — циклические (n, k_0)- и (n, k)-словари, порождаемые $g(x)$ и $m(x)g(x)$ соответственно, где $m(x)$ — многочлен степени k_0-k, имеющий, по меньшей мере, один корень порядка ε. Если минимальное расстояние между любыми двумя словами из D_0 равно d_0, то индекс неуязвимости s_m смежного класса D с n-последовательностью $g(x)$ в качестве лидера смежного класса ограничен неравенством

$$s_m \geqslant \begin{cases} d_0-|m|, & |m| \leqslant \min(n-d_0,\ \varepsilon-1); \\ 2d_0-n, & n-d_0 \leqslant |m| \leqslant \varepsilon-1. \end{cases}$$

Доказательство. Если $0<m<\varepsilon$, то все корни многочлена $x^{n-m}-1$ имеют порядок меньший, чем ε, и $x^{n-m}-1$ не является делителем $m(x)$. Следовательно, n-последовательность, представляемая $c(x)(x^{n-m}-1)$ [где $c(x)=g(x)$], и поэтому также слово, представляемое $w'(x)=c(x)(x^{n-m}-1)-w(x)$ (где $w(x)$ соответствует слову из D), входят в D_0 и не входят в D. Пусть $p_m(x)$ префикс длины m из D. Тогда, так как любое слово из D, содержащее этот префикс, должно отличаться от любого другого слова из D_0, по меньшей мере, в d_0 местах, то самое большее $\min(m, n-d_0)$ соответствующих коэффициентов многочленов $x^{n-m}p_m(x)$ и $w'(x)$ могут быть равными. Таким образом, $c(x)(x^{n-m}-1)-w(x)-x^{n-m}p_m(x)$ является многочленом, по меньшей мере, с $d_0-\min\{m, n-d_0\}$ ненулевыми коэффициентами. Любой стык слов должен поэтому отличаться от любого кодового слова, по крайней мере, на эту величину, и теорема доказана. ■

Рассмотрим в качестве примера двоичные БЧХ коды с $n-15$ (ср. с § 13.5). Классы сравнений степеней и соответствующие многочлены приведены в табл. 14.2 [в таблице приведены делители $x^{15}-1$ над $GF(2)$].

Таблица 14.2

Классы сравнений многочленов	Соответствующие многочлены	Порядок корней многочленов
1 2 4 8	$p_1(x)=x^4+x+1$	15
3 6 12 9	$p_2(x)=x^4+x^3+x^2+x+1$	5
5 10	$p_3(x)=x^2+x+1$	3
7 14 13 11	$p_4(x)=x^4+x^2+1$	15
0	$p_5(x)=x+1$	1

Таким образом, если положить $g(x)=p_1(x)p_2(x)$ и $m(x)=p_3(x)$, то получим смежный класс БЧХ (15,5)-кода с минимальным расстоянием 7 и с индексом неуязвимости $s_m \geqslant 5-|m|$ для всех $|m| \leqslant 2=\varepsilon-1$. Аналогично определяя $g(x)=p_1(x)p_2(x)$ и $m(x)=p_4(x)$, получим (15,3)-код с минимальным расстоянием, не меньшим 5, и индексом неуязвимости $s_m \geqslant 5-|m|$ для всех $m \leqslant 4$.

Заметим, что минимальное расстояние d между любыми двумя словами из D может быть, а может и не быть большим d_0 в зависимости от многочлена $m(x)$. Может оказаться, что в некоторых классах более важно иметь большее ε, чем получить d, превосходящее d_0 и $m(x)$ должно быть выбрано в соответствии с этим.

Параметры некоторых БЧХ кодов, которые получаются с помощью конструкции, указанной в теореме 14.15, и имеют смежные классы, обладающие свойством неуязвимости, сведены в табл. 14.3, где $\hat{s}_m$ — верхняя граница для s_m [см. (14.34)].

Этот подход особенно уместен в случае кодов Рида—Соломона (§ 13.5). Пусть $g(x)=\prod_{i=1}^{n-k-1}(x-\alpha_i)$, $n=q-1$ и α — примитивный элемент $GF(q)$, и пусть, например, $m(x)=(x-\alpha^{n-k})$; при этом получаем (n, k)-код с минимальным расстоянием $n-k+1$ и индексом неуязвимости

$$s_m \geqslant \begin{cases} n-k-|m|, & |m| \leqslant \min(k, \varepsilon-1); \\ n-2k, & k \leqslant |m| \leqslant \varepsilon-1, \end{cases} \tag{14.36}$$

Таблица 14.3

n	k	d	d_0	ε	s_m	$\lvert m\rvert_{\text{макс}}$	$\hat{s}_m$
15	11	3	1	15	$1-\lvert m\rvert$	0	$4-\lvert m\rvert$
15	9	3	3	3	$3-\lvert m\rvert$	2	$6-\lvert m\rvert$
15	7	5	3	5	$3-\lvert m\rvert$	2	$8-\lvert m\rvert$
15	5	7	5	3	$5-\lvert m\rvert$	2	$10-\lvert m\rvert$ $\quad\lvert m\rvert\leqslant 5$
							5 $\quad\lvert m\rvert\geqslant 5$
15	3	5	5	15	$5-\lvert m\rvert$	4	$12-\lvert m\rvert$ $\quad\lvert m\rvert\leqslant 3$
							9 $\quad\lvert m\rvert\geqslant 3$
15	2	10	6	15	$6-\lvert m\rvert$	5	$13-\lvert m\rvert$ $\quad\lvert m\rvert\leqslant 2$
							11 $\quad\lvert m\rvert\geqslant 2$
15	1	15	7	15	$7-\lvert m\rvert$	6	13

где ε — порядок элемента α^{n-k}. Если $\varepsilon\geqslant n-k+1$, то получающийся код имеет индекс неуязвимости на всех m позициях, лежащий на верхней границе (14.34). Например, код Рида—Соломона (4, 1) над $GF(5)$, порождаемый многочленом $g(x)=(x-3)(x-4)(x-2)$, имеет смежный класс D[с $c(x)=(x-3)(x-4)$] с индексом свободы от запятой $s=2:D=\{2310,\ 3421,\ 4032,\ 0143,\ 1204\}$.

Ограничивая рассмотрение векторами, принадлежащими некоторому циклическому $(n,\ k_0)$-коду, мы, очевидно, ограничиваем множество возможных лидеров смежных классов, которые могли бы быть использованы. Преимущества этого подхода, по существу, связаны с общими свойствами циклических кодов, а именно, с тем, что, во-первых, их математическая структура приводит к возможности получения результатов и, во-вторых, относительно легко порождаются лидеры смежных классов. Тем не менее иногда полезны также другие подходы. Один из них изучается в оставшейся части этого параграфа.

Лемма 14.2. Если D является циклическим $(n-k)$-кодовым словарем с минимальным расстоянием d и если δ_m из первых (меньших по порядку) $n-m$ коэффициентов многочлена $c(x)(x^{n-m}-1)$ [т. е. многочлена $\sum_{i=0}^{n-m-1}(c_{i+m}-c_i)x^i$] отличны от нуля, то смежный класс D с лидером смежного класса $\mathbf{c}=\{c_0,\ c_1,\dots,\ c_{n-1}\}$ имеет индекс s_m, для которого справедлива граница снизу:

$$s_m\geqslant\min\{\delta_m,\ d-|m|-\delta_m\}. \tag{14.37}$$

Доказательство. Независимо от многочлена $p_m(x)$ многочлен (14.35) должен иметь самое меньшее δ_m и самое большее $m+\delta_m$ ненулевых коэффициентов. Так как любой ненулевой многочлен кодового слова должен иметь самое малое d ненулевых коэффициентов и так как для циклических кодов $s_m=s_{n-m}$, то неравенство (14.37) справедливо для всех m, $1\leqslant m\leqslant n-1$ ■.

Поэтому представляет интерес следующая лемма.

Лемма 14.3. Пусть

$$c(x)=\sum_{i=\delta_0}^{[(\delta-1)/2]} x^{i(\mu+1)-\delta_0}+x^{n-1}, \tag{14.38}$$

где $\delta_0=\begin{cases}0, & \delta \text{ четное;}\\ 1, & \delta \text{ нечетное}\end{cases}$ и где $\mu<\left(n-\left[\frac{\delta}{2}\right]\right)\Big/\left[\frac{\delta+1}{2}\right]$ (здесь $[\delta]$ обозначает целую часть α). Тогда ровно δ среди первых $n-m$ коэффициентов многочлена $(x^{n-m}-1)c(x)$ не равны нулю для всех m из отрезка $1\leqslant m\leqslant\mu$.

Доказательство. Рассмотрим многочлен

$$(x^{n-m}-1)c(x)=\sum_{i=\delta_0}^{[(\delta-1)/2]}\left(x^{i(\mu+1)-\delta_0-m)}-x^{i(\mu+1)-\delta_0}\right)+$$
$$+x^{n-m-1}-x^{n-1}.$$

Так как $m\leqslant\mu<\left(n-\left[\frac{\delta}{2}\right]\right)\Big/\left[\frac{\delta+1}{2}\right]$, то наибольший показатель степени под знаком суммы меньше, чем $n-m-1$. Более того, никакие два слагаемых под знаком суммы не имеют одинаковых показателей, если $1\leqslant m\leqslant\mu$. Поэтому, когда δ нечетное, суммирование дает $2[(\delta-1)/2]=\delta-1$ ненулевых коэффициентов, соответствующих показателям из отрезка $(0, n-m-1)$. Когда δ четное, $\delta_0=0$ и среди δ слагаемых под знаком суммы только первое имеет показатель, лежащий вне требуемого отрезка. Так как коэффициент при x^{n-m-1} не равен нулю, то ровно δ среди первых $n-m$ коэффициентов $(x^{n-m}-1)c(x)$ не равны нулю в каждом из этих двух случаев. ■

Теорема 14.16. Любой циклический (n, k)-код с минимальным расстоянием d может быть сделан неуязвимым при синхронизации с индексом $s_m=s$ на всех позициях $|m|\leqslant\mu$, где

$$\mu\leqslant\min\left\{d-2s,\ \left(n-1-\left[\frac{s}{2}\right]\right)\Big/\left[\frac{s+1}{2}\right]\right\}. \tag{14.39}$$

Доказательство. Используя лидер смежного класса, представляемый многочленом $c(x)$ из леммы 14.3 согласно лемме 14.2, получим, что $s\geqslant\min\{\delta, d-\mu-\delta\}$. Таким образом, если $\mu\leqslant d-2\delta$, то для индекса неуязвимости имеем $s\geqslant\delta$. Вторая граница сверху для μ является условием, которое накладывается леммой 14.3. ■

Заметим, что когда $s=1$, то $c(x)=x^{n-1}$. Соответствующий лидер смежного класса делает, конечно, любой циклический (n, k)-код неуязвимым при синхронизации на всех позициях m, $|m|\leqslant n-k-1$, хотя теорема 14.16 гарантирует это только для случая $|m|\leqslant d-2$. Когда $s=2$, то $c(x)=1+x^{n-1}$, и получающийся код будет неуязвимым с индексом 2 на всех позициях m при $|m|\leqslant d-4$. Если

$d \geqslant [n/2]+4$, то такой код поэтому является кодом без запятой с индексом 2. Однако эта конструкция никогда не может гарантировать получение индекса свободы от запятой, большего 2, так как μ должно быть меньше, чем $(n-[s/2])/[s+1)/2]$.

Лидер смежного класса, представляемый многочленом $c(x)$ (14.38), не является единственным, который имеет требуемые свойства. Однако очевиден принцип, лежащий в основе его выбора; ненулевые коэффициенты многочленов $c(x)$ и $x^{n-m}c(x)$ не пересекаются при всех $|m| \leqslant \mu$. В результате величина δ_m (лемма 14.2) постоянна при всех m в указанном интервале независимо от поля, над которым определен многочлен $c(x)$. Хотя условие постоянства δ_m легко достичь, оно не обязательно является наиболее эффективным. Заметим, например, что δ_m может увеличиваться с уменьшением m без нежелательного влияния на индекс неуязвимости [см. (14.37)]. Этот факт часто можно с выгодой использовать, особенно, если $c(x)$ подогнано к заданному коду или к классу кодов. Однако независимо от многочленов $c(x)$ максимальный индекс неуязвимости, гарантируемый этой конструкцией, не может быть больше $(d-|m|)/2$ [см. опять (14.37)]. Таким образом, конструкция того типа, который описан в теореме 14.15, в общем предпочтительна всегда, когда d_0 больше, чем $(d+|m|)/2$.

Для целей сравнения результаты, полученные при применении конструкции из теоремы 14.16 к БЧХ (15, k)-кодам, сведены в табл. 14.4 (ср. с табл. 14.3). [В качестве лидера смежного класса используется (14.38)]. Величины $|m|_{\text{макс}}$, указанные для случая $s=1$, являются возможными, как показывает теорема (14.7).

Таблица 14.4

n	k	d	s	$\lvert m\rvert_{\text{макс}}$
15	11	3	1	3
15	9	3	1	5
15	7	5	1	7*
15	7	5	2	1
15	5	7	1	7*
15	5	7	2	3
15	5	7	3	1
15	1	15	2	7*
15	1	15	4	6
15	1	15	5	4
15	1	15	6	3
15	1	15	7	1

Примечание. Звездочкой отмечены коды без запятой

14.10. Коды, исправляющие ошибки синхронизации

При введении понятия синхронизационной неуязвимости было отмечено, что если синхронизированная система вдруг теряет синхронизацию, то это часто происходит из-за сдвига лишь на небольшое число позиций в каком-либо из направлений. В силу этой причины, как было указано, иногда полезно выбирать лидер смежного класса так, чтобы гарантировать большой индекс неуязвимости на всех позициях $|m|\leqslant\mu$ для некоторого относительно малого μ вместо того, чтобы пытаться сделать код «свободным от запятой». По этой же самой причине выгодно также иметь возможность определять не только то, что произошла ошибка синхронизации, но также и то, какая именно позиция m в действительности наблюдается. Это позволило бы исправлять ошибки за один шаг, избегая использования иногда довольно длительной процедуры поиска. Коды, которые дают возможность декодеру исправлять синхронизационные ошибки таким способом, называют кодами, *исправляющими ошибки синхронизации*[1]. В этом параграфе рассмотрено несколько методов построения таких кодов.

Подход, предложенный в предыдущих параграфах для обнаружения синхронизационных ошибок, состоял в требовании, чтобы все стыки кодовых слов вида $a_{m+1}a_{m+2}\ldots a_n b_1 b_2\ldots b_m$ отличались в возможно большем числе позиций от всех кодовых слов для всех представляющих интерес значений $|m|$. Очевидным обобщением этого условия, которое необходимо для того, чтобы синхронизационные ошибки были исправлены или обнаружены, является требование, чтобы все такие стыки с $m=m_1$ отличались по возможности в большей степени не только от всех правильных кодовых слов, но и от всех других стыков с $m\neq m_1$ опять-таки для всех представляющих интерес значений $|m|$. Если расстояние между любыми двумя стыками, соответствующими различным значениям m, $|m|\leqslant\mu$, больше или равно t, то величина и направление любой синхронизационной ошибки величины $|m|\leqslant\mu$ могут быть правильно распознаны всегда, когда ошибочными были не более $[(t+1)/2]$ соответствующих символов. В этом состоит основная идея конструкций, которые рассматриваются ниже[2].

---

[1] Эти коды не следует путать с кодами, исправляющими вставки и выпадения. Если причиной синхронизационной ошибки является вставка или выпадение одного или большего числа символов в некотором кодовом слове, то методы, которые исследуются здесь, будут применимы к первой принимаемой n последовательности, которая следует за такой ошибкой. Никакой попытки исправить слово, содержащее вставленные или выпавшие символы, предприниматься не будет. *(Прим. авт.)*.

[2] Иногда в литературе используется другое название — коды, *восстанавливающие* синхронизацию, — для обозначения кодов, которые указывают если не величину синхронизационной ошибки, то, по крайней мере, знак этой ошибки (т. е. такие коды способны отличать синхронизационные ошибки на $+m_1$ символов и на $-m_2$ символов для всех $0<m_1$, $m_2\leqslant\mu$).

(Продолжение на стр. 443)

Первая конструкция в точности совпадает с той, которая описана в теореме 14.15. Если максимальное значение $|m|$ ограничить еще больше, то получающиеся коды могут быть использованы для исправления синхронизационных ошибок, как показывает следующая теорема.

Теорема 14.17. Пусть D_0, D, $g(x)$, $m(x)$, ε и d_0 определены так же, как в теореме 14.15; рассмотрим вновь смежный класс D с вектором, представленным $g(x)$ в качестве лидера смежного класса. Расстояние между любым стыком слов, начинающимся на любой позиции m_1, и любым стыком слов на любой другой позиции m_2 для такого словаря

$$t \geqslant \begin{cases} d_0 - 2|m|, & |m| \leqslant n - d_0; \\ 3d_0 - 2n, & |m| \geqslant n - d_0, \end{cases}$$

где $|m| = \max\{|m_1|, |m_2|\} < \varepsilon/2$.

Доказательство. Любой стык слов, начинающийся на любой позиции m, может быть представлен многочленом

$$Q_m(x) = x^{n-m} c(x) + x^{n-m} p_m(x) + q_m(x) = x^{n-m} c(x) + w(x) + \\ + x^{n-m} p'_m(x) = x^{n-m} c(x) + w'(x) + q'_m(x). \qquad (14.40)$$

[Обозначения те же, что в (14.17), т. е. $c(x) = g(x)$ — многочлен лидера смежного класса; $w(x)$ и $w'(x)$ — слова из D; $p_m(x)$ и $p'_m(x)$ — многочлены степени $m-1$ или меньшей, соответствующие префиксам из D, а $q_m(x)$ и $q'_m(x)$ — многочлены степени $n-m-1$ или меньшей, соответствующие суффиксам из D.] Расстояние между стыком слов, начинающимся на позиции m_1, и стыком слов на позиции m_2 равно числу ненулевых коэффициентов многочлена $Q_{m_1}(x) - Q_{m_2}(x)$. Чтобы упростить доказательство, предположим, что $m_1 \leqslant n/2$ и $m_2 \leqslant n/2$. Минимальное расстояние между двумя стыками слов при этом предположении дает нижнюю границу для расстояния в общем случае, что легко проверить. При этом

$$Q_{m_1}(x) - Q_{m_2}(x) = c(x)\, x^{n-m}\left(1 - x^{|m_1|+|m_2|}\right) + w''(x) + \\ + x^{n-m_1} p'_{m_1}(x) - q'_{m_2}(x) \qquad (14.41)$$

где $w''(x)$ — слово из D, а $|m| = \min(m, n-m)$. Если $|m_1| + |m_2| < \varepsilon$, то первое выражение и поэтому сумма первых двух выражений в (14.41) соответствуют словам из D_0, не принадлежащим D (см. доказательство теоремы 14.15), и, таким образом, они имеют по меньшей мере d_0 ненулевых коэффициентов. Тогда, поступая так же, как и в доказательстве теоремы 14.15, получаем, что

Так как, по-видимому, различие как в избыточности, так и в сложности реализации кодов, исправляющих ошибки в синхронизации, и кодов, восстанавливающих синхронизацию, невелико, то лишь первые из них будут рассмотрены здесь сколько-нибудь подробно. (*Прим. авт.*).

расстояние t между рассматриваемыми стыками слов ограничено неравенством

$$t \geqslant \begin{cases} d_0 - (|m_1| + |m_2|), & |m_1|, \quad |m_2| \leqslant n - d_0; \\ d_0 - 2(n - d_0), & |m_1|, \quad |m_2| \leqslant n - d_0; \end{cases} \tag{14.42}$$

и теорема доказана. ■

В случае (n, k)-кодов Рида—Соломона $d_0 = n - k$ и, если $\varepsilon > 2\mu$, то

$$t \geqslant \begin{cases} n - k - 2\mu, & \mu \leqslant k; \\ n - 3k, & \mu \geqslant k. \end{cases}$$

Этот результат нельзя существенно улучшить, как показывает следующая теорема.

Теорема 14.18. Пусть D' — смежный класс циклического (n, k)-кодового словаря. Тогда минимальное расстояние t_μ между любым стыком его слов на позиции μ и любым стыком на позиции — μ ограничено неравенством

$$t_\mu \leqslant \begin{cases} n - k - 2\mu, & \mu \leqslant k, (n-k)/2 \\ n - 3k, & k \leqslant \mu \leqslant (n-k)/2; \\ 2(\mu - k), & (n-k)/2, k \leqslant \mu; \\ 0, & (n-k)/2 \leqslant \mu \leqslant k. \end{cases}$$

Доказательство. Рассмотрим два вектора

$$\mathbf{v}_1 = a_{n-\mu+1}, \quad a_{n-\mu+2}, \ldots, \quad a_n, \quad b_1, \quad b_2, \ldots \quad b_{n-\mu};$$

$$\mathbf{v}_2 = c_{\mu+1}, \quad c_{\mu+2}, \ldots, \quad c_n, \quad d_1, \quad d_2, \ldots, \quad d_\mu,$$

где $\mathbf{a} = (a_{n-\mu+1}, \ldots, a_n)$ и $\mathbf{c} = (c_{\mu+1}, \ldots, c_n)$ — суффиксы, а $\mathbf{b} = (b_1, \ldots, b_{n-\mu})$ и $\mathbf{d} = (d_1, \ldots, d_\mu)$ — префиксы из D'. Так как D' является смежным классом циклического кода, то имеется некоторая μ-последовательность $\mathbf{a}$, такая, что первые $\delta = \min(\mu, k)$ компонент $\mathbf{v}_1$ совпадают с первыми δ компонентами $\mathbf{v}_2$. Аналогично и по той же самой причине последние δ компонент $\mathbf{v}_2$ могут совпадать с последними δ компонентами $\mathbf{v}_1$. Наконец, так как $(n-\mu)$-последовательность $\mathbf{b}$ является пока произвольной, можно выбрать ее так, чтобы ее первые $\gamma = \min(k, n - 2\mu)$ компонент равнялись соответствующим компонентам $\mathbf{v}_2$. Таким образом, $t_\mu \leqslant n - 2\delta - \gamma$, и отсюда следует утверждение теоремы.

Следствие. Никакой циклический (n, k)-код не способен исправлять все возможные синхронизационные ошибки, если не выполнено условие $k \leqslant [(n-1)/3]$.

Доказательство. Если $k \geqslant n/3$, то $(n-k)/2 \leqslant k$. Следствие сразу же становится очевидным, если положить $\mu = (n-k)/2$, так как в этом случае согласно теореме 14.18 $t_\mu = 0$.

Это условие в противоположность тому, которое было найдено ранее для требования свободы от запятой (§ 14.4), является необходимым но не достаточным, как показывает полное рассмотрение $(4,1)$-кода $\begin{pmatrix}0000\\1111\end{pmatrix}$. Тем не менее любой циклический (n, k)-код имеет смежный класс, который исправляет ошибки синхронизации на всех позициях $|m| \leqslant (n-k-2)/2$ (ср. с теоремой 14.18), как показывает следующая теорема.

Теорема 14.19. Пусть D' будет смежным классом циклического (n, k)-кодового словаря D с лидером смежного класса, представляемым $c(x) = 1 + x^{n-1}$. Тогда все стыки слов из D' на позиции m_1 отличаются от всех стыков на позиции m_2 при всех $m_1 \neq m_2$, $\mu \triangleq \max\{|m_1|, |m_2|\} \leqslant (n-k-2)/2$.

Доказательство. Как уже было замечено, минимальное расстояние между двумя стыками слов, одно из которых на позиции m_1, $0 < m_1 \leqslant n/2$, а другое на позиции m_2, $n/2 < m_2 \leqslant n$, равно минимальному числу ненулевых коэффициентов в многочлене (14.41). Два стыка слов могут быть равными при этом только тогда, когда многочлен

$$x\, c(x) \left(1 - x^{m_1 + |m_2|}\right) + x p'_{m_1}(x) - x^{m_1+1} q'_{m_2}(x)$$

представляет собой кодовое слово из D. Но если $c(x) = 1 + x^{n-1}$, то этот многочлен имеет степень $m_1 + |m_2| + 1$ или меньшую. Если, следовательно, $n - m_1 - |m_2| - 2 \geqslant k$, то он не может представлять собой слово из D, если только оно не является нулевым словом, что невозможно здесь из-за того, что коэффициент при x^0, очевидно, не равен нулю. По существу, такое же доказательство применимо, когда $0 \leqslant m_2 < m_1 < n/2$ и когда $n/2 \leqslant m_1 < m_2 \leqslant n$, что доказывает теорему 1).

Лидер смежного класса, использованный в теореме 14.16, также появляется в словаре с некоторой способностью к исправлению ошибок синхронизации.

Теорема 14.20. Пусть D — смежный класс циклического (n, k)-кода с минимальным расстоянием d и с лидером смежного класса того вида, который представляется многочленом (14.38), но где μ заменено на 2μ. Тогда любой стык слов этого словаря на любой позиции m_1 отделен расстоянием, по меньшей мере, равным t, от любого стыка слов на любой другой позиции $m_2 \neq m_1$ для всех $|m_1|, |m_2| \leqslant \mu$, где

$$\mu \leqslant \min\left\{\frac{d-2t-1}{2},\quad \frac{n-[(t+3)/2]}{2\,[(t+2)/2]}\right\}.$$

Доказательство. Повторяя во всех существенных деталях доказательства лемм 14.2 и 14.3, легко проверить, что:

---

1) Заметим, что с помощью такого же доказательства можно показать, что D' обладал бы способностью к *восстановлению* синхронизации при всех $\mu \leqslant (n-k-1)/2$, если $c(x) = 1$ (или x^{n-1}). *(Прим. авт.)*.

1. Расстояние между стыком слов на позиции m_1 и стыком на позиции m_2 ограничено снизу неравенством

$$t_{m_1, m_2} \geqslant \min\{\delta_{m_1, m_2}, d-\mu'-\delta_{m_1, m_2}\},$$

где

$$\mu' \triangleq \begin{cases} |m_1|, & 0 \leqslant m_2 < m_1 \leqslant \dfrac{n}{2} \text{ или } \dfrac{n}{2} \leqslant m_1 < m_2 \leqslant n; \\ |m_1|+|m_2|, & 0 < m_1 \leqslant \dfrac{n}{2} < m_2 \leqslant n \end{cases}$$

и $\delta_{m_1 m_2}$ — число ненулевых членов в первых $n-\mu'$ коэффициентах многочлена

$$Q(x) \triangleq \begin{cases} (x^{n-m_1}-x^{n-m_2})\,c(x), & 0 \leqslant m_2 < m_1 \leqslant \dfrac{n}{2}; \\ (1-x^{n-|m_1|+|m_2|})\,c(x), & \dfrac{n}{2} \leqslant m_1 < m_2 \leqslant n; \\ (x^{n-m_1-|m_2|}-1)\,c(x), & 0 < m_1 \leqslant \dfrac{n}{2} < m_2 \leqslant n; \end{cases}$$

$c(x)$, очевидно, лидер смежного класса.

2. Если $c(x)$ определяется согласно (14.38), но с заменой везде μ на 2μ, то $\delta-1 \leqslant \delta_{m_1, m_2} \leqslant \delta$; $|m_1|, |m_2| \leqslant \mu < \dfrac{n-[\delta/2]}{2[(\delta+1)/2]}$.

Объединяя эти два утверждения, находим, что

$$t \triangleq \min_{m_1 m_2} t_{m_1, m_2} \geqslant \min\{\delta-1, d-2\mu-\delta\},$$

где $\mu \triangleq \max\{|m_1|, |m_2|\} \leqslant \dfrac{n-1-[\delta/2]}{2[(\delta+1)/2]}$.

Сформулированное в теореме утверждение получается теперь, если потребовать, чтобы $d-2\mu-\delta \geqslant \delta-1$. ■

До сих пор мало было сказано относительно методов использования возможностей линейных кодов исправлять и обнаруживать ошибки в синхронизации, рассмотренные в этом и нескольких предыдущих параграфах настоящей главы. В действительности относительная предпочтительность различных возможных подходов в значительной мере зависит от физических ограничений. Наиболее удовлетворительное решение в случае, когда проблема синхронизации в основном состоит в первоначальном входе в синхронизм и когда потеря синхронизации происходит не часто, не обязательно будет таким же, как в случае, когда потеря синхронизации происходит довольно регулярно.

В первой из этих ситуаций может оказаться целесообразным, чтобы декодер работал всегда так, как будто бы синхронизация является верной. Справедливость этого предположения можно было бы затем проверить с помощью измерения расстояния между каждой принятой n-последовательностью и соответствующим выходом декодера, что предлагалось в § 14.5. Если используемый код имеет достаточно большой индекс неуязвимости на рассматриваемой позиции, то этот факт должен был бы отразиться в таком изменении статистики измеряемого расстояния, которое поддавалось бы наблюдению. Если на основе этих наблюдений обнаруживается синхронизационная ошибка, то можно начать (или продолжить) синхронизационный поиск. Этот метод исследуется далее в § 14.16 и 14.17. Если используемый код может как исправлять синхронизационные ошибки, так и обнаруживать их, то с помощью дальнейших наблюдений, по-видимому, можно было бы определить правильную синхронизацию слов без какого-либо поиска, хотя реализация этого метода могла бы быть сложной.

Когда потеря синхронизации происходит относительно часто, только что описанный статистический подход может оказаться неэффективным; среднее время между потерями синхронизации может оказаться недостаточным для построения надежного решения. В этом случае более разумным методом было бы разделение множества принимаемых n-последовательностей на два или более подмножеств. Если принятая n-последовательность попадает в подмножество n-последовательностей, которые достаточно похожи на настоящие кодовые слова, то можно предположить, что синхронизация правильная, и приступить к операции декодирования. Если нет, то можно было бы вновь начать поиск или в зависимости от подмножества, к которому принадлежит принятая n-последовательность, можно было бы немедленно произвести исправление синхронизации. Этот подход в противоположность предыдущему почти неизбежно уменьшает возможности кода исправлять ошибки в синхронизации. Другими словами, для достижения той же самой синхронизационной характеристики должны быть использованы более избыточные коды. Этого следовало ожидать, так как от кода требуется больше, чем просто способность исправлять (или обнаруживать) ошибки. В общем случае этот последний тип синхронизации может привести к значительным трудностям при реализации. Однако, как и при обычном исправлении ошибок, связанные с реализацией задачи часто можно значительно упростить, используя алгебраическую структуру предлагаемого кода, за счет, возможно, более низкой способности к исправлению или обнаружению ошибок в синхронизации. Этот подход изучается в следующем параграфе.

14.11. Алгебраически синхронизируемые коды, исправляющие ошибки

Для того чтобы проиллюстрировать применение алгебраических методов для одновременного исправления ошибок замещения и синхронизационных ошибок, рассмотрим еще раз код, определенный в теореме 14.15. Алгоритм декодирования будет следующим. Декодер вначале вычитает последовательность, соответствующую лидеру смежного класса, из каждой принятой n-последедовательности и декодирует результат так, как будто бы она была словом из словаря D_0 (определение терминов см. в теореме 14.15). Синдром декодированного слова затем вычисляется по отношению к словарю D и используется для определения как величины, так и направления синхронизационной ошибки.

Для того чтобы понять, как и при каких условиях работает этот алгоритм, предположим, что декодер в действительности начинает декодирование на позиции m. Принятое слово после того, как из него был вычтен лидер смежного класса, представляется многочленом

$$c(x)\left(x^{n-m}-1\right)+w(x)-x^{n-m}p_m(x)+e(x),$$

где $e(x)$ — многочлен, представляющий ошибки замещения, а $c(x)=g(x)$ — порождающий многочлен кода D_0. Пусть число ненулевых коэффициентов в $e(x)$ (т. е. число ошибок) равно e. Тогда, если $e+m\leqslant(d_0-1)/2$, то выход декодера будет иметь вид $c(x)(x^{n-m}-1)w(x)$. (Напомним, что декодирование производится так, как если бы принятая n-последовательность была словом из D_0.) Синдром $s_m(x)$ получается с помощью деления этого многочлена на $g(x)m(x)$. Таким образом,

$$s_m(x)=\left\{c(x)\left(x^{n-m}-1\right)+w(x)\right\}_{m(x)\,g(x)}=\left\{x^{n-m}\right\}_{m(x)},$$

где последнее выражение означает остаток после деления $(x^{n-m}-1)$ на $m(x)$. Предположим, что β — корень $m(x)$ порядка ε. Тогда $s_m(\beta)=\beta^{n-m}-1$. Очевидно, что никакие два синдрома $s_{m_1}(x)$ и $s_{m_2}(x)$, $m_1\neq m_2$ не могут быть равными, если $|m_1|+|m_2|<\varepsilon$; следовательно, каждая синхронизационная ошибка, величина которой не превышает $\mu\leqslant(\varepsilon-1)/2$, приводит к однозначному синдрому. Для того чтобы завершить операцию декодирования, нужно лишь изменить синхронизацию декодера в соответствии с этим синдромом. Если синдром равен нулю, то первоначальный выход декодера представлял собой правильное слово [в предположении, что действительное число ошибок не было большим $(d_0-1)/2-|m|$] и процесс декодирования может продолжаться рассмотрением следующего принятого слова.

Один из минусов этого алгоритма декодирования состоит в уменьшении эффективного хэмминговского расстояния словаря D от значения d до значения d_0 (или, что эквивалентно, в уменьшении размерности D_0 от значения k_0 до значения k). Конечно, можно декодировать принятое слово, как слово из D, а не как слово из D_0, и избежать этой потери в синхронизационной характеристике. Однако такой способ значительно усложняет решение относительно того, была или не была потеряна синхронизация, и фактически заставляет декодер выносить статистическое решение по этому поводу, как было описано ранее. Причина этого состоит в том, что если принимаемый поток символов декодируется в соответствии с D, то все корректируемые комбинации ошибок в действительности будут исправлены. Лишь среднее расстояние между первоначальными n-последовательностями и декодированными вариантами и, возможно, число неисправленных комбинаций ошибок будут указывать на возможность синхронизационной ошибки.

Однако эта трудность реализации всех синхронизационных потенциальных возможностей алгебраически синхронизируемых кодов, исправляющих ошибки, иногда может быть преодолена, как показывает следующая конструкция. Пусть D_0 — циклический (n, k)-код, порождаемый $g(x)$ и имеющий минимальное расстояние $d_0=d$, и пусть D — укороченный циклический $[n-(2\mu+1), k-(2\mu+1)]$-код, получаемый при оставлении в D_0 только тех слов, которые начинаются $\mu+1$ нулями и оканчиваются μ нулями, и дальнейшем отбрасывании этих нулей. Пусть далее D' — смежный класс D с лидером смежного класса, представляемым многочленом $c(x)=w_0(x)$, где $w_0(x)$ какое-либо слово из D_0, начинающееся $(\mu+1)$-последовательностью 00...01 и оканчивающееся μ-последовательностью 00...0. [Заметим, что такое слово должно существовать в силу молчаливого предположения о том, что $2(\mu+1)\leqslant k$.] Тогда верно следующее утверждение.

Теорема 14.21. Слова из словаря D', определенного в предыдущем абзаце, можно декодировать алгебраически, так что: 1) все комбинации ошибок, содержащие $(d-1)/2$ или меньшее число ошибок, будут исправлены, когда декодер находится в синхронизме с принимаемой последовательностью слов, и 2) если декодер в действительности начинает декодирование на позиции m, то при $|m|\leqslant\mu$ как величина, так и направление этой синхронизационной ошибки будут определены при условии, что число ошибок замещения не больше, чем $[(d-1)/2]-2|m|-1$.

Доказательство. Алгоритм декодирования будет следующим:

1) Принимаемая последовательность символов разбивается на блоки длины $n-2(\mu+1)$.

2. Каждый блок снабжается префиксом в виде $(\mu+1)$-последовательности 00...01 и суффиксом в виде μ-последовательности 00...0, и результирующая n-последовательность декодируется в соответствии с D_0.

3. Если ее первый ненулевой символ появляется на i-й позиции, то декодированное слово циклически сдвигается на $\mu+1-i$ позиций вправо (если $i\leqslant\mu+1$) или на $i-\mu-1$ позиций влево (если $i>\mu+1$) и из результата вычитается лидер смежного класса.

4. Если первые $(\mu+1)$ и последние μ символов результирующей n-последовательности являются нулевыми, то эти символы опускаются и остаток принимается в качестве декодированного слова. Кроме того, выносится решение, что декодер начинает декодирование на позиции $m=\mu+1-i$ и производится соответствующая подстройка до того, как декодируется следующая $(n-2\mu-1)$-последовательность.

5. Если условия п. 4 не выполняются, то результат регистрируется в виде отказа при декодировании и декодер переходит к следующей $(n-2\mu-1)$-последовательности без какой-либо подстройки синхронизации.

Чтобы проверить, что характеристика этого декодера является такой, как указано в теореме, рассмотрим ситуацию, когда декодер начинает декодирование на позиции $m \leqslant \mu$. Образуемая декодером n-последовательность может быть представлена многочленом

$$Q(x) = x^{\mu} + x^{\mu+1} q_{m+2\mu+1}(x) + x^{n-\mu-m} p_m(x) + e(x),$$

где $q_l(x)$ и $p_l(x)$ представляют собой $(n-l)$-символьный суффикс из D и l-символьный префикс из D' соответственно, а $e(x)$ — комбинация ошибок замещения. Так как

$$x^{\mu} + x^{\mu+1} p'_m(x) + x^{\mu+1+m} q_{m+2\mu+1}(x) = w(x) + w_0(x),$$

где $w(x)$ слово из D; $p'_m(x)$ — m-символьный префикс из D' и $w_0(x)$ было определено ранее, то получаем

$$Q(x) = x^{\mu} + x^{n-m}(w(x) + w_0(x)) - x^{\mu-m} - x^{\mu-m+1} p'_m(x) +$$
$$+ x^{n-\mu-m} p_m(x) + e(x).$$

Следовательно, выходом декодера будет слово, представляемое многочленом $w'(x) = x^{n-m}[w(x) + w_0(x)]$ при условии, что число ненулевых коэффициентов в многочлене $Q(x) - w'(x)$ не больше, чем $(d-1)/2$. И это заведомо будет так, если $e + 2m + 1 \leqslant (d-1)/2$, $m \neq 0$, или если $e \leqslant (d-1)/2$, $m = 0$, где e — число ошибок замещения. Тогда первый ненулевой символ в декодированном слове появится на позиции $i = \mu + 1 - m$ и как синхронизационная ошибка, так и принятое слово будут правильно опознаны. То же самое доказательство, очевидно, применимо в случае, когда декодер начинает декодирование на позиции $m \geqslant n - \mu$, и теорема доказана. ■

Таким образом, укороченные циклические коды имеют смежные классы, дающие возможность исправлять синхронизационные ошибки без ухудшения способности исправлять синхронные ошибки замещения. Дело в том, что нужно выбрать лидер смежного класса так, чтобы синхронизационные ошибки выглядели как ошибки замещения в символах, которые в действительности никогда не передавались. Однако к этому утверждению следует сделать две оговорки. Во-первых, укороченный код, на самом деле, может иметь минимальное расстояние, большее, чем у первоначального циклического кода; если это так, то алгоритм декодирования, рассмотренный здесь, не использует этого обстоятельства. Во-вторых, уязвимость процедуры исправления синхронизационных ошибок по отношению к ошибкам замещения увеличивается вдвое быстрее с ростом $|m|$ по сравнению с предыдущей конструкцией.

Третья конструкция для алгебраически декодируемых кодов, исправляющих синхронизацию, которая будет описана здесь, представляет любопытный контраст по отношению к предыдущему методу; вместо того чтобы укоротить циклический код, мы его фактически удлиним. Эта конструкция хотя и увеличивает избыточность кода без увеличения его способности к исправлению ошибок замещения, но приводит к коду, который является не более уязвимым по отношению к ошибкам замещения при неверном синхронизме, чем в случае, когда декодер находится в правильном синхронизме с принятой последовательностью. Идея этой конструкции станет понятной, если заметить, что уязвимость по отношению к ошибкам замещения для кодов, описанных в теоремах 14.15 и 14.17, увеличивается с ростом m только тогда, когда стык слов составлен из двух различных кодовых слов [т. е. когда $p_m(x) \neq 0$]. Этот дефект можно устранить, если снабжать каждое передаваемое слово подходящими «буферными последовательностями» в качестве суффикса и префикса.

А именно, пусть D, D_0, $g(x)$, $m(x)$, d_0 и ε определяются так же, как в теоремах 14.15 и 14.17. Построим новый $(n+m_r+m_l, k)$ — словарь D_s, содержащий слова вида

$$\mathbf{w}_s = w_{n-m_l} w_{n-m_l+1} \dots w_{n-1} w_0 w_1 \dots w_{n-1} w_0 w_1 \dots w_{m_r-1}, \qquad (14.43)$$

где $\mathbf{w} = (w_0 w_1 \dots w_{n-1})$ — слово из смежного класса D, имеющего лидер смежного класса, представляемый многочленом $g(x)$. Словарь D_s отличается от этого смежного класса лишь повторением его последних m_l символов и его первых m_r символов.

Пусть теперь алгоритм декодирования будет следующим. Сначала отбрасываются m_l начальных и m_r конечных символов принятого $(n+m_l+m_r)$-символьного кодового слова. Затем вычитается лидер смежного класса, и остающееся n-символьное слово декодируется так, как если бы оно было словом из D_0. Если синхронизация является верной и если во время передачи произошло $(d_0-1)/2$ или менее ошибок замещения, то переданное слово будет декодировано верно. Но, кроме этого, если синхронизация была ошибочной, но не более чем на m_r символов вправо или m_l символов влево, то вход декодера [если не считать $(d_0-1)/2$ или меньшее число ошибок замещения, которые исправляются] будет некоторой циклической перестановкой некоторого слова из смежного класса D, порожденного $g(x)$. Доказательство теоремы 14.17 прямо применимо в настоящем случае, однако здесь префиксные многочлены $p_m(x)$ и суффиксные многочлены $q_m(x)$ равны нулю. Повторяя доказательство теоремы 14.17 с этим видоизменением, получаем, следовательно, приводимый ниже результат.

Теорема 14.22. Определенный выше $(n+m_r+m_l, k)$-словарь D_s может исправлять вплоть до $(d_0-1)/2$ ошибок замещения и одновременно исправлять все синхронизационные ошибки из отрезка $-m_l \leqslant m \leqslant m_r$, $m_l+m_r<\varepsilon$.

14.12. Синхронизируемые коды, исправляющие пачки ошибок

Не должно удивлять, что коды, построенные для борьбы с пачками ошибок, должны быть эффективными также и при обнаружении и исправлении синхронизационных ошибок. Действительно, если код циклический, синхронизационная ошибка сама может быть представлена, как пачка ошибок. Если использовать смежный класс этого кода с лидером смежного класса, представленным $c(x)=1+x^{n-1}$ (где n — длина кодового слова), то можно гарантировать, что любая пачка ошибок из-за ошибочной синхронизации будет выглядеть для декодера как концевая «круговая» пачка, т. е. как пачка, которая начинается суффиксом, а оканчивается префиксом того же самого кодового слова. При синхронной работе та же самая комбинация ошибок наблюдалась бы обычно только тогда, когда появились бы две последовательные пачки, разделенные менее чем длиной кодового слова, что, по-видимому, является маловероятным событием. Так как циклические коды, исправляющие пачки ошибок, тем не менее способны исправлять концевые круговые ошибки точно так же, как и обычные пачки ошибок, то эта неиспользованная способность может быть применена для исправления или обнаружения синхронизационных ошибок. Докажем, в частности, следующее утверждение.

Теорема 14.23. Пусть D будет циклическим (n, k)-словарем, способным обнаруживать все пары пачек ошибок с общей длиной, не большей b_d [1]), и пусть D' будет смежным классом D с лидером смежного класса, представленным многочленом $c(x)=1+x^{n-1}$. Тогда, если исключена возможность появления концевых круговых пачек ошибок, то декодер для D' можно построить так, чтобы либо обнаруживать одновременное появление пачки длины b, или меньшей, и синхронизационной ошибки величины μ, или меньшей, при любых $\mu+b\leqslant b_d-2$, либо исправлять синхронизационную ошибку величины, не большей $\mu\leqslant\max\{(b_d-4)/2,\ (n-k-2)/2\}$, и пачку ошибок длины $b\leqslant b_d/2$, где $\mu+b\leqslant b_d-2$ при условии, что они не появляются одновременно.

Доказательство. Доказательство этого результата следует почти непосредственно из рассуждений, приведенных выше. Декодер может декодировать принятую последовательность символов, вычитая из каждой последовательной n-последовательности лидер смежного класса и декодируя результат в соответствии с D. Если он начинает декодирование на позиции m, то в отсутствие пачки ошибок n-последовательность на входе декодера представляется многочленом

$$c(x)\left(x^{n-m}-1\right)+w(x)-x^{n-m}p_m(x),\quad 0\leqslant m\leqslant\frac{n}{2},$$

или $c(x)\left(x^{n-m}-1\right)+w(x)-q_m(x),\ \dfrac{n}{2}\leqslant m\leqslant n$ [ср. с (14.40)]. В любом случае влияние синхронизационной ошибки состоит в том, что вводится концевая круговая пачка длины $|m|+2$ с непересекающимися множествами пачек, соответствующих каждому m, $|m|<(n-1)/2$. Отсюда сразу же следует, что одновременное появление этих двух типов ошибок можно обнаружить, если $|m|+2+b\leqslant$

---

[1]) Напомним, что согласно §13.10 $b_d\geqslant n-2k+1$ для любого циклического (n, k)-кода. (*Прим. авт.*).

$\leqslant b_d$, и что любая из ошибок может быть исправлена, если она появляется одна и если как $|m|+2$, так и b ограничены сверху величиной $b_d/2$ [ср. с § 13.10]. Ошибки этих двух типов можно различить, так как синхронизационная ошибка всегда приводит к концевой круговой пачке, в то время как согласно предположению обычная пачка ошибок такого типа появиться не может. То, что синхронизационные ошибки величины $(n-k-2)/2$ в действительности могут исправляться при отсутствии других ошибок, уже было доказано в теореме 14.19. Однако для того, чтобы были исправлены синхронизационные ошибки бо́льшие, чем $(b_d/2)-2$, необходимо, чтобы соответственно возросла способность к исправлению пачек ошибок так, чтобы пачки и синхронизационные ошибки все еще можно было различить. Это требование, очевидно, удовлетворяется, если $\mu+2+b\leqslant b_d$, где $\mu=\max|m|$. ■

Очевидно, что результаты предыдущих параграфов, относящиеся к способности линейных кодов исправлять и обнаруживать ошибки в синхронизации, когда имеются произвольные ошибки замещения, применимы также в случае, когда ошибки появляются пачками. Иногда в случае, когда ошибки появляются только пачками, эти результаты можно усилить, как показывает следующая теорема.

Теорема 14.24. Определенный в теореме 14.15 словарь, представляющий собой смежный класс, способен исправлять все пачки ошибок длины b и меньшей и одновременно исправлять все синхронизационные ошибки величины, не большей $\mu<\varepsilon/2$, если $\mu+b\leqslant(n-3k_0+2)/2$.

Доказательство. Повторяя доказательство теоремы 14.17, получаем, что любые два стыка слов — один, начинающийся на позиции m_1, а другой — на позиции m_2 —, содержащие пачки ошибок длины b_1 и b_2 соответственно, будут отличаться, если

$$c(x)\,x^{n-m_1}\left(1-x^{|m_1|+|m_2|}\right)+w''(x)+x^{n-m_1}\,p'_{m_1}(x)-q'_{m_2}(x)+$$
$$+\,b_1(x)+b_2(x)\not\equiv 0 \tag{14.44}$$

для любого слова $w''(x)$ из D. Обозначения здесь совпадают с теми, которые использованы в ф-ле (14.41) с тем исключением, что два многочлена $b_1(x)$ и $b_2(x)$ представляют собой пачки ошибок длины b_1 и b_2. Как и в теореме 14.17, предположим, что $0\leqslant m_1\leqslant\leqslant n/2<m_2\leqslant n$. То же доказательство лишь с небольшими видоизменениями (в действительности при более слабых условиях) справедливо также для других случаев. Теперь для любых $|m_1|+|m_2|\leqslant\varepsilon$ (где ε определено в теореме 14.15) первый член и, следовательно, сумма первых двух членов в ф-ле (14.44) представляют собой слова из D_0, но не из D. Таким образом, условие (14.44) нарушится только тогда, когда

$$P(x)\triangleq x^{n-m_1}\,p'_{m_1}(x)-q'_{m_2}(x)+b_1(x)+b_2(x)=w_0(x), \tag{14.45}$$

где $w_0(x)$ — некоторое ненулевое слово из D_0 (но не из D). Так как $x^{n-m_1}p'_{m_1}(x)-q'_{m_2}(x)$ можно интерпретировать как пачку длины

$m_1+|m_2|$, то условие (14.45) нельзя удовлетворить во всех случаях, кроме того, когда некоторое ненулевое слово из D_0 может быть представлено в виде суммы трех пачек ошибок с длинами $|m_1|+|m_2|$, b_1 и b_2. Но если $|m_1|+|m_2|+b_1+b_2 \leqslant n-3k_0+2$, то, по крайней мере, один из интервалов, отделяющих две из этих пачек ошибок, содержит k_0 или большее число символов. Так как D_0 является циклическим (n, k_0)-словарем, то лишь нулевое слово может содержать последовательность k_0 или большего числа подряд идущих нулей. Если $|m_1|$, $|m_2| \leqslant \mu$ и если b_1, $b_2 \leqslant b$, то (14.45) нельзя удовлетворить при указанных условиях, и теорема доказана.

Если словарь из предыдущей теоремы определяется над двоичным полем, то в некоторых случаях можно повысить границу для максимально дозволенной суммы $b+\mu$. Предположим, что многочлен $P(x)$, определенный ф-лой (14.45), содержит в целом γ «единиц». Очевидно, что $P(x)$ не может представлять собой ненулевое слово из D_0, кроме случая, когда $\gamma \geqslant d_0$, где d_0 — вес слова минимального веса из D_0. Но если $P(x)$ является словом из D_0, то $(1+x)P(x)$ также будет словом и если $P(x)$ содержит в целом γ единиц, то $(1+x)P(x)$ может иметь самое большее $2(|m_1|+|m_2|+b_1+b_2-\gamma)+6$ единиц поскольку символ в $(1+x)P(x)$ является единицей только тогда, когда в качестве одного из соответствующих символов $P(x)$ или $xP(x)$ появляется нуль, а в качестве другого — единица. Для того чтобы $(1+x)P(x)$ представляло собой слово из D_0, должно быть либо $\gamma=n$, либо $2(|m_1|+|m_2|+b_1+b_2-\gamma) \geqslant d_0-6$. Если как $P(x)$, так и $(1+x)P(x)$ должны представлять слова из D_0, то

$$|m_1|+|m_2|+b_1+b_2 \geqslant \min\{3(d_0-2)/2,\ n\} = 3(d_0-2)/2.$$

Это последнее равенство следует непосредственно из границы (13.11), т. е. поскольку здесь $k_0 \geqslant 2$, то $n \geqslant 3d_0/2$. Тем самым доказана следующая теорема.

Теорема 14.25. Если словарь в теореме 14.24 определяется над $GF(2)$, то он может исправлять все пачки ошибок длины, меньшей или равной b, и все синхронизационные ошибки величины, меньшей или равной μ, где $\mu+b \leqslant (3d_0-7)/4$.

14.13. Индекс свободы от запятой в кронекеровском произведении кодов, кронекеровской сумме кодов и в каскадных кодах

Один из полезных методов построения кодов, имеющих большие индексы свободы от запятой, состоит в составлении кронекеровского произведения либо кронекеровской суммы (см. § 13.7) пары меньших кодов, каждый из которых является кодом без запятой с индексом, по меньшей мере, равным единице. Вывод границы для индекса свободы от запятой в образующемся коде, выраженной через индексы составляющих кодов, является первой из задач этого параграфа. Результаты приведены в следующей теореме.

Теорема 14.26. Пусть $M \times m$ и $N \times n$ — матрицы $\mathbf{A}_m$ и $\mathbf{B}_n$ представляют собой два линейных кодовых словаря, каждый из которых содержит состоящее из единиц кодовое слово 11...1. Пусть $\mathbf{c}_m$ будет m-последовательностью, а $\mathbf{d}_n$ n-последовательностью, такими, что соответствующие коды $\mathbf{A}_m + \mathbf{c}_m$ и $\mathbf{B}_n + \mathbf{d}_n$ будут иметь индексы свободы от запятой s_m и s_n. (Матрица $\mathbf{A}_m + \mathbf{c}_m$ представляет собой словарь, который получается с помощью почленного сложения в поле $GF(q)$, над которым определены обе матрицы $\mathbf{A}_m$ и $\mathbf{B}_n$, n-последовательности $\mathbf{c}_m$ с каждой строкой $\mathbf{A}_m$ и аналогично для матрицы $\mathbf{B}_n + \mathbf{d}_n$). Далее пусть $\mathbf{C}_{mn}$ представляет собой словарь, порождаемый кронекеровским произведением порождающих матриц $\mathbf{A}_m$ и $\mathbf{B}_n$, и пусть $\mathbf{D}_{mn}$ будет кронекеровской суммой $\mathbf{A}_m$ и $\mathbf{B}_n$. Тогда индекс свободы от запятой s_{mn} в словарях $\mathbf{C}_{mn} + (\mathbf{c}_m \boxplus \mathbf{d}_n)$ и $\mathbf{D}_{mn} + (\mathbf{c}_m \boxplus \mathbf{d}_n)$ ограничен неравенством $s_{mn} \geqslant \min(ns_m, ms_n)$. Здесь mn-последовательность $\mathbf{c}_m \boxplus \mathbf{d}_n$ является кронекеровской суммой $\mathbf{c}_m = (\gamma_1 \gamma_2 \ldots \gamma_m)$ и $\mathbf{d}_n = (\delta_1 \delta_2 \ldots \delta_n)$, т. е. $\mathbf{c}_m \boxplus \mathbf{d}_n = (\gamma_1 + \mathbf{d}_n, \gamma_2 + \mathbf{d}_n, \ldots, \gamma_m + \mathbf{d}_n)$, где $\gamma_i + \mathbf{d}_n = (\gamma_i + \delta_1, \gamma_i + \delta_2, \ldots, \gamma_i + \delta_n)$.

Доказательство. Теорему довольно легко доказать, отметив следующие два свойства любого слова $\mathbf{w}$ из $\mathbf{C}_{mn}$ или $\mathbf{D}_{mn}$:

1) $\mathbf{w}$ имеет вид $\mathbf{w} = \mathbf{b}_{i_1} \mathbf{b}_{i_2} \ldots \mathbf{b}_{i_m}$,

где $\mathbf{b}_i$ — слова $\mathbf{B}_n$;

2) символы ω_{in+j}, $i = 0, 1, \ldots, m-1$, слова $\mathbf{w} = (\omega_1 \omega_2 \ldots \omega_{mn})$ образуют кодовое слово из $\mathbf{A}_m$ при любом $\mathbf{w}$ и любом $j = 1, 2, \ldots, n$. [Оба эти утверждения отражают просто то обстоятельство, что если $\mathbf{w}$ является словом из линейного словаря D, определенного над полем $GF(q)$, и если D содержит состоящее из одних единиц слово $\mathbf{w}_0 = (11\ldots1)$, то как $\alpha\mathbf{w}$, так и $\alpha\mathbf{w}_0 + \mathbf{w}$ являются словами из D при любом α из $GF(q)$.] Прямыми следствиями этих двух утверждений будут следующие утверждения, справедливые для любого слова $\mathbf{w}'$ из $\mathbf{C}_{mn} + (\mathbf{c}_m \boxplus \mathbf{d}_n)$ или $\mathbf{D}_{mn} + (\mathbf{c}_m \boxplus \mathbf{d}_n)$:

1а) $\mathbf{w}'$ имеет вид $\mathbf{w}' = \mathbf{b}'_{i_1} \mathbf{b}_{i_2} \ldots \mathbf{b}'_{i_m}$, где $\mathbf{b}'_i$ слова из $\mathbf{B}_n + \mathbf{d}_n$;

2а) символы ω'_{in+j}, $i = 0, 1, \ldots, m-1$, слова $\mathbf{w}' = (\omega'_1 \omega'_2 \ldots \omega'_{mn})$ образуют кодовое слово из $\mathbf{A}_m + \mathbf{c}_m$ при любом $\mathbf{w}'$ и любом $j = 1, 2, \ldots, n$.

Пусть теперь $\mathbf{w}$ и $\mathbf{w}'$ — слова либо из $\mathbf{W} = \mathbf{C}_{mn} + (\mathbf{c}_m \boxplus \mathbf{d}_n)$, либо из $\mathbf{W} = \mathbf{D}_{mn} + (\mathbf{c}_m \boxplus \mathbf{d}_n)$; рассмотрим любой стык последовательности $\mathbf{w}\mathbf{w}'$, начинающийся $(i+1)$-м символом $\mathbf{w}$ и оканчивающийся i-м символом $\mathbf{w}'$. Если $i \neq 0$ по модулю n, то этот стык является последовательностью из m n-последовательностей, каждая из которых могла бы появиться в качестве стыка слов $\mathbf{B}_n + \mathbf{d}_n$. В соответствии с этим все эти стыки слов должны отличаться самое меньшее в s_n местах от любого слова из $\mathbf{B}_n + \mathbf{d}_n$ и, по меньшей мере, ms_n символов любого такого стыка должны отличаться от соответствующих символов в любом слове из $\mathbf{W}$. Аналогично, если $i = 0$ по модулю n $(i = \nu n, \nu \neq 0)$, символы $\omega_{\nu n+j}\, \omega_{(\nu+1)n+j}, \ldots, \omega_{(m-1)n+j} \omega'_j \omega'_{n+j}, \ldots, \omega'_{(\nu-1)n+j}$ составляют (при каждом $j = 1, 2, \ldots, n$) m-последовательность, которая могла бы появиться в качестве стыка двух слов из

$\mathbf{A}_m + \mathbf{c}_m$. Таким образом, каждая из этих n m-последовательностей должна отличаться, по меньшей мере, в s_m местах от любого слова из $\mathbf{A}_m + \mathbf{c}_m$ и соответствующий стык $\mathbf{ww}'$ должен отличаться от любого слова из $\mathbf{W}$, по меньшей мере, в ns_m местах. Так как все нетривиальные стыки любых двух слов из $\mathbf{C}_{mn} + (\mathbf{c}_m \boxplus \mathbf{d}_n)$ или $\mathbf{D}_{mn} + (\mathbf{c}_m \boxplus \mathbf{d}_n)$ были учтены в этих рассуждениях, то получаем, что

$$s_{mn} \geqslant \min[ns_m, ms_n], \tag{14.46}$$

и теорема доказана. ■

В утверждении этой теоремы требуется, чтобы оба составляющих кода содержали слово, состоящее из единиц. Это нужно для того, чтобы гарантировать, что все стыки кодовых слов, появляющихся в кронекеровской сумме или кронекеровском произведении словарей, могли бы также появляться в составляющих словарях. Очевидно, что если $\widetilde{D}$ — словарь, содержащийся в D, и $\widetilde{D}$ используется вместо D в определении кронекеровской суммы или произведения словарей, то получающийся словарь имеет индекс свободы от запятой, по меньшей мере, такой же, как словарь, определенный с помощью D. Таким образом, нет противоречия между предположениями теорем 14.26 и 13.18. (Напомним, что последняя требовала, чтобы слова одного из двух словарей, входящих в кронекеровскую сумму, имели максимальный вес, меньший, чем n.) Заметим также, что если, по крайней мере один из двух составляющих словарей в кронекеровской сумме или если оба словаря в кронекеровском произведении содержат кодовое слово, состоящее из единиц, то такое же слово содержит получающийся словарь. В соответствии с этим процесс можно итерировать; кронекеровское произведение и кронекеровская сумма словарей без запятой могут быть использованы для того, чтобы породить еще большие кронекеровское произведение и сумму словарей без запятой.

Аналогичный результат справедлив для каскадных кодов. Пусть (n_1, k_1)-код D_1, определенный над $GF(q^{k_2})$ и имеющий индекс свободы от запятой s_1. Аналогично пусть (n_2, k_2)-код D_2 над $GF(q)$, имеющий индекс свободы от запятой s_2. Каскадный код образуется при однозначном сопоставлении с каждым элементом $GF(q^{k_2})$ слова из D_2. Требование, чтобы D_1 и D_2 были кодами без запятой, ничего не меняет при рассмотрении синхронизирующих свойств этого кода. Однако каскадный код теперь также будет кодом без запятой с индексом свободы от запятой (в терминах q-ичных символов):

$$s_{n_1 n_2} \geqslant \min\{n_1 s_2, d_2 s_1\}, \tag{14.47}$$

где d_2 — минимальное расстояние между двумя любыми словами из D_2. Рассмотрим опять стык слов, начинающийся $(i+1)$ символом одного слова и оканчивающийся i-м символом другого. Если $i=0$ по модулю n_2 (но не по модулю $n_1 n_2$), то свобода от запятой D_1 гарантирует, что этот стык слов будет отличаться от любого кодового слова, по меньшей мере, s_1 q^{k_2}-ичными символами и, следовательно, по меньшей мере, $s_1 d_2$ q-ичными символами. Если $i \neq 0$ по модулю n_2, то расстояние между стыком слов и любым правильным словом будет, очевидно, по меньшей мере, равно n_1s_2.

В действительности это свойство каскадных кодов довольно несущественно, так как цель каскадирования состоит не просто в порождении больших q-ичных кодов, а дополнительно в получении более удобного декодирования (ср. с § 13.9). Предположим, что словари без запятой D_1 и D_2 объединяются с помощью каскадирования или с помощью образования их кронекеровского произведения или кронекеровской суммы. Тогда любая последовательность слов из этого объединенного словаря также является последовательностью слов из D_2 (или D_1 в зависимости от порядка, в котором объединяются эти два словаря). Синхронизация слов, таким образом, может быть выполнена в два этапа; первый этап состоит в определении начальных символов слов из D_2, а второй — в разрешении остающейся неоднозначности. Первый этап поиска можно производить так, как если бы использовался один словарь D_2. Второй этап после этого будет состоять в поиске по n_1 остающимся позициям, основанном на свойстве отсутствия запятой в D_1. В результате общее число позиций, которое нужно рассмотреть, будет равно n_1+n_2, а не n_1n_2, как в случае, когда эта подструктура не учитывается.

В заключение этого параграфа суммируем некоторые известные результаты, касающиеся свойств свободы от запятой кодов Рида—Маллера первого порядка, упомянутых в § 13.7. Напомним, что эти коды могут порождаться с помощью последовательного кронекеровского суммирования матрицы $\mathbf{D}_1=\begin{bmatrix}0 & 0\\ 0 & 1\end{bmatrix}$ с самой собой и последующего присоединения к полученному словарю его дополнения. Таким образом, словарь D_i представляется матрицей

$$\mathbf{D}_i=\begin{bmatrix}\mathbf{D}_{i-1} & \mathbf{D}_{i-1}\\ \mathbf{D}_{i-1} & \mathbf{D}_{i-1}\end{bmatrix}$$

и $(2^{k-1}, k)$ — словарь Рида—Маллера представляет собой просто $D_{k-1}\cup\overline{D}_{k-1}$. Тот же самый словарь D_{k-1} в равной мере можно определить с помощью кронекеровской суммы любой из пар матриц $\mathbf{D}_j$ и $\mathbf{D}_{k-1-j}$, $1\leqslant j\leqslant k-1$, что легко проверить. Поэтому для того, чтобы показать существование кодов Рида—Маллера без запятой всех размерностей, необходимо лишь указать их для меньших размерностей. Фактически, если словарь $D_1\cup\overline{D}_1$ можно было бы сделать свободным от запятой, то теорема 14.26 гарантировала бы, что то же самое справедливо для кодов Рида—Маллера всех бо́льших размерностей.

К сожалению, словарь $D_1\cup\overline{D}_1$ содержит все двоичные 2-последовательности и, очевидно, не может быть сделан свободным от запятой. Более того, граница из теоремы 14.13 показывает, что никакой из словарей $D_{k-1}\cup\overline{D}_{k-1}$ не может быть словарем без запятой при любых $k<4$. Код Рида—Маллера с $k=4$ также не может быть сделан свободным от запятой, как легко проверить, используя методы § 14.3. Например, ранг матрицы **M**, определенной соотношением (14.6), равен 8, если $m=5$. Чтобы показать существование кодов Рида—Маллера без запятой для всех размерностей $k \geqslant 5$, мы должны получить их для размерностей $k=5$, 6, 7 и 8 (например, кронекеровская сумма словаря D_4 с самим собой дает словарь D_8, а $D_8 \cup \overline{D_8}$ является словарем Рида—Маллера с $k=9$). Такие коды были найдены и с помощью вычислительной машины были вычислены их индексы свободы от запятой. Результаты вместе с верхними границами s' для этих индексов приведены ниже:

k	s	s'
5	2	2
6	7	7
7	16	22
8	34	56

(14.48)

Первые две границы сверху ($k=5$ и 6) были получены при использовании методов, описанных в § 14.8, последние две — с помощью двух различных методов. Все эти границы более точны, чем граница (14.24). Лидеры смежных классов, дающие оптимальные словари с $k=6$, были найдены методом перебора (с помощью вычислительной машины) снова с использованием результатов § 14.8.

14.14. Фазовые коды без запятой

Синхронизируемость фазовых кодов (§ 13.11) также может быть улучшена превращением словарей в коды без запятой. Мерой, которая представляет интерес в этом случае, является корреляция между словом и стыком слов, а не хэмминговское расстояние между ними. Это означает, что если $\mathbf{y}=(y_1 y_2 \ldots y_n)$ — вектор показателей степени принятой n-последовательности, а $\mathbf{x}^\mu=(x^\mu{}_1 x^\mu{}_2 \ldots x^\mu{}_n)$ — вектор показателей степени кодового слова, то рассматривается *асинхронный коэффициент корреляции*

$$\rho_\mu(\mathbf{y}) = \frac{1}{n} \sum_{\nu=1}^{n} e^{(2\pi i/r)\left(x^\mu_\nu - y_\nu\right)} . \qquad (14.49)$$

Так как декодер по предположению является корреляционным приемником, то эти (искаженные шумом) коэффициенты составляют основу для его решений относительно принятого слова. Синхронизация слов, очевидно, легче всего получается по самой последовательности данных, если множество коэффициентов корреляции $\rho_\mu(\mathbf{y})$ в случае, когда n-последовательность $\mathbf{y}$ представляет правильное кодовое слово, значительно отличается от коэффициентов корреляции в случае, когда она является стыком двух кодовых слов.

Следующая теорема иллюстрирует соотношение между этими коэффициентами корреляции и индексом свободы от запятой, связанным с кодовой степенной группой (определения терминов см. в § 13.11).

Теорема 14.27. Пусть C — некоторый смежный класс группы G, состоящей из n-последовательностей целых чисел по модулю r и пусть каждая из n-последовательностей из C определяет показатели степени слова из фазового кодового словаря D. Предположим, что словарь C, рассматриваемый как словарь n-символьных r-ичных слов, имеет индекс свободы от запятой s. Тогда

$$\max_{\mathbf{y},\,\mu} \operatorname{Re}\{\rho_\mu(\mathbf{y})\} \leqslant 1 - \frac{s}{n}\left(1-\cos\frac{2\pi}{r}\right),$$

где $\rho_\mu(\mathbf{y})$ определяется соотношением (14.49). Более того, если G содержит n-последовательность из единиц $\mathbf{g}_0 = (11\ldots1)$, то

$$\max_{\mathbf{y},\,\mu} |\rho_\mu(\mathbf{y})| \leqslant \left[1-2\frac{s}{n}\left(1-\frac{s}{n}\right)\left(1-\cos\frac{2\pi}{r}\right)\right]^{1/2}.$$

Доказательство. Первое из этих утверждений очевидно, так как

$$\max_{\mathbf{y},\,\mu} \operatorname{Re}\{\rho_\mu(\mathbf{y})\} \leqslant \operatorname{Re}\left\{\frac{n-s}{n}+\frac{s}{n}e^{2\pi i/r}\right\} = 1-\frac{s}{n}\left(1-\cos\frac{2\pi}{r}\right) < 1. \tag{14.50}$$

Доказательство второго утверждения почти столь же просто. Во-первых, заметим, что $|\rho_\mu(\mathbf{y})| = |\rho_\mu(\mathbf{y}-\gamma\mathbf{g}_0)|$ для любого целого γ. Пусть γ будет значением (или одним из значений), принимаемым наибольшим числом (скажем, l) компонент $\mathbf{y}-\mathbf{x}^\mu$. Тогда

$$|\rho_\mu(\mathbf{y}-\gamma\mathbf{g}_0)| \leqslant \begin{cases} \left|\dfrac{l}{n}+\dfrac{n-l}{n}e^{2\pi i/r}\right|, & l > \dfrac{n}{2}; \\[2ex] \dfrac{1}{2}\left|1+e^{2\pi i/r}\right|, & l \leqslant \dfrac{n}{2}, \end{cases} \tag{14.51}$$

так как $|\rho_\mu(\mathbf{y}-\gamma\mathbf{g}_0)|$, очевидно, достигает наибольшего значения, когда аргументы $y_\nu - x_\nu^\mu - \gamma$, $\nu = 1, 2, \ldots, n$, по возможности близки друг к другу. Поскольку G содержит $\mathbf{g}_0$ и является кодом без запятой с индексом s, то $l \leqslant n-s$ и отсюда следует указанная в теореме верхняя граница для $|\rho_\mu(\mathbf{y})|$. (Эта граница может быть сделана более точной, если s больше, чем $n/2$.) ■

Как следствие, результаты, касающиеся кодов без запятой и полученные в предыдущих параграфах, имеют смысл и здесь. Однако следует подчеркнуть, что, кроме как в двоичном и в троичном фазовокогерентном случаях, эти две меры являются различными и что наилучшие коды без запятой не обязательно порождают наилучшие фазовые коды.

Фазовыми кодами, которые представляют наибольший интерес, несомненно являются ортогональные и r-ортогональные фазовые коды, рассмотренные в § 13.11. Они соответствуют в высшей степени избыточным кодам, исправляющим ошибки, и, как следовало бы ожидать, можно найти такие коды, асинхронные коэффициенты корреляции которых имеют значения, значительно меньшие единицы. Как было показано в § 13.11, с помощью метода кронекеровского произведения могут быть построены r-ортогональные фазовые коды с произвольными размерностями. Поэтому представляет интерес следующая теорема относительно максимума асинхронного коэффициента корреляции кронекеровского произведения словарей.

Теорема 14.28. Пусть A_m и B_n — словари фазовой кодовой группы (смежные классы), состоящие из M и N слов по m и n символов в каждом соответственно; пусть оба они определены над множеством символов $\{\exp(2\pi i\gamma/r)\}$. Пусть далее смежные классы степенной группы обоих этих словарей будут смежными классами групп, которые содержат m- (n)-последовательность из единиц $(11...1)$. Наконец, пусть ρ_m и ρ_n — асинхронные коэффициенты корреляции, имеющие максимальные абсолютные величины в этих двух словарях. Тогда

$$|\rho_{mn}| \leqslant \max\{|\rho_m|, |\rho_n|\},$$

где ρ_{mn} — асинхронный коэффициент корреляции кронекеровского произведения этих двух словарей, имеющий максимальное абсолютное значение.

Доказательство прямо следует из доказательства теоремы 14.26. Кронекеровское произведение фазовых кодов соответствует кронекеровской сумме смежных классов их степенных групп (т. е. соответствует смежному классу, который получается с помощью сложения каждого из элементов кронекеровской суммы их групп с кронекеровской суммой соответствующих им лидеров смежного класса. Таким образом, если $i\neq 0$ по модулю n, то $|\rho_{mn}|\leqslant|\rho_n|$, а если $i=0$ по модулю n, то $|\rho_{mn}|\leqslant|\rho_m|$, и теорема доказана.

Далее выводится полезная граница снизу для асинхронного коэффициента корреляции, достижимого на ортогональных словарях (и в силу этого на r-ортогональных словарях).

Теорема 14.29. Пусть D является словарем ортогонального фазового кода с n словами по n символов в каждом, имеющим максимальный (по абсолютной величине) асинхронный коэффициент корреляции ρ_n. Тогда $|\rho_n|\geqslant 1/\sqrt{n}$.

Доказательство. Обозначая через $\{\xi^n\}$ множество слов из D, а через η любой стык любых двух слов D, получим

$$\eta = \sum_{\mu=1}^{n} \rho_\mu \xi^\mu. \tag{14.52}$$

Это следует в силу того, что пространство n-последовательностей, определенных над комплексным полем, является линейной оболочкой множества ортогональных векторов ξ^μ. Более того, так как $\xi^\nu\cdot\eta=n\rho_\nu$, то

$$\frac{1}{n}(\eta\cdot\eta) = 1 = \sum_{\mu=1}^{n}|\rho_\mu|^2. \tag{14.53}$$

Предположим теперь, что $\max\limits_{\mu}|\rho_\mu| < 1 \sqrt{n}$. Тогда $\sum\limits_{\mu=1}^{n} |\rho_\mu|^2 < 1$, что приводит к противоречию, доказывая тем самым теорему[1]).

В двоичном случае $|\rho_n| = |1-(2s/n)|$, где s — индекс свободы от запятой; в этом случае обе меры эквивалентны. Коды Рида—Маллера первого порядка для меры, рассматриваемой в этом параграфе, являются биортогональными, так что рассмотрения предыдущего параграфа, касающиеся $(2^{k-1}, k)$-кодов Рида—Маллера без запятой, прямо применимы здесь. Величина асинхронных коэффициентов корреляции, которая достигается на этих кодах, может непосредственно быть получена из (14.48).

Если $r=p$ является простым числом, большим 3, то легко показать, что при всех $k \geqslant 2$ существуют p-ичные p-ортогональные (p^{k-1}, k)-коды с асинхронными коэффициентами корреляции, имеющими максимальные абсолютные значения, меньшие единицы. Если существуют такие коды для $k=2$, то существование всех других кодов гарантируется теоремой о кронекеровском произведении кодов. Чтобы проверить, что коды с $k=2$ можно сделать свободными от запятой, необходимо лишь заметить, что код, порождаемый с помощью всех линейных комбинаций над $GF(p)$ двух p-последовательностей

$$\begin{bmatrix} 0 & 1 & 2 & 3 \ldots (p-1) \\ 1 & 1 & 1 & 1 \ldots 1 \end{bmatrix}, \tag{14.54}$$

является циклическим. Следовательно, результаты § 14.4 показывают, что смежный класс, который получается с помощью сложения какого-либо ненулевого целого числа с последним (или первым) столбцом этого кода, является свободным от запятой. Это справедливо при $k \leqslant (n-1)/2$, т. е. при $p \geqslant 5$. Действительно, когда $p > 7$, можно использовать лидер смежного класса, указанный в теореме 14.16, чтобы сделать эти коды свободными от запятой с индексом 2. Несомненно, что большие индексы свободы от запятой возможны для больших значений p.

14.15. Фазовые последовательности Баркера

Предположим, что нужно передать информацию по гауссовскому каналу с помощью последовательностей ФТ символов $s_\nu(t) = \sqrt{2}\sin[\omega_c t + (2\pi/r)\xi_\nu]$, $\xi_\nu \in (0, 1, \ldots, r-1)$ длительность T_s секунд и что синхронизация должна быть получена с помощью определения на приемном конце периодически передаваемой последовательности $\{z_\nu \quad (t) = \sqrt{2}\sin(\omega_c t + (2\pi/r)x_\nu), \quad (\nu-1)T_s < t < \nu T_s\}$, $\nu = 1, 2, \ldots, n$, представляющей собой запятую. (Последовательность $\{x_\nu\}$ будем называть *фазовой запятой.*). Если по предположению информация состоит из взаимонезависимых символов, равномерно распределенных на алфавите сигнала, то рассуждения § 14.6 можно обобщить и считать, что адекватной мерой здесь является *апериодический коэффициент корреляции*

---

[1]) Эта граница вместе с некоторыми усовершенствованиями составляет основу для последних двух верхних границ, приведенных в (14.48). (*Прим. авт.*).

$$\lambda_k = \sum_{\nu=1}^{n-k} \zeta_\nu \zeta^*_{\nu+k}, \tag{14.55}$$

где $\zeta_\nu = e^{(2\pi i/r)x_\nu}$. «Хорошей» синхронизирующей последовательностью в этом случае могла бы быть такая, для которой по определению $|\lambda_k| \leqslant 1$ для всех $k=1, 2, \ldots, n-1$. Это является очевидным аналогом условия, введенного в § 14.6.

Параметр λ_k тождествен параметру c_k из § 14.6, когда $r=2$, и в фазовокогерентном случае, когда $r=3$. Таким образом, в этих двух ситуациях непосредственно применимы результаты § 14.6. Несколько последовательностей баркеровского типа (последовательностей, для которых $|\lambda_k| \leqslant 1$ для всех k) произвольной длины известны для значений r, больших 2. Если $r = r_1 r_2$, то над r-ичным алфавитом, очевидно, могут быть построены последовательности, которые, по крайней мере, столь же хороши, как и те, которые можно получить либо над r_1-ичным, либо над r_2-ичным алфавитами. Для этого просто можно использовать фазовую последовательность $\{r_2 x_\nu\}$, где $\{x_\nu\}$ — фазовая запятая над r_1-символьным алфавитом. Таким образом, если $r=4$, то последовательности, удовлетворяющие ограничению $|\lambda_\nu| \leqslant 1$ для всех k, существуют для длин $n=2, 3, 4, 5, 7, 11$ и 13, поскольку существуют двоичные последовательности для всех этих длин. Кроме того, существует 4-ичная последовательность с $|\lambda_k| \leqslant 1$, $1 \leqslant k \leqslant n-1$ для $n=15$. Известны другие недвоичные ФТ последовательности, удовлетворяющие этому ограничению, когда $r=6$, для всех n из отрезков $2 \leqslant n \leqslant 13$.

Вообще говоря, приемлемые фазовые последовательности баркеровского типа можно получить, выбирая некоторую циклическую перестановку псевдошумовой последовательности. Для любой фазовой последовательности справедливы неравенства:

$$\max_{0<k<n} |\lambda_k + \lambda_{n-k}| \geqslant \operatorname*{ave}_{0<k<n} |\lambda_k + \lambda_{n-k}| = \frac{1}{n-1} \left| \sum_{k=1}^{n} \sum_{j=1}^{n} z_k z^*_{k+j} - n \right| =$$

$$= \frac{1}{n-1} \left\{ \left| \sum_{k=1}^{n} z_k \right|^2 - n \right\} \geqslant -[n/(n-1)]. \tag{14.56}$$

Псевдошумовые фазовые последовательности, лежащие на этой границе, представляют собой, по-видимому, естественный источник последовательностей баркеровского типа.

Другим методом построения длинных фазовых последовательностей баркеровского типа является использование кронекеровской суммы двух более коротких фазовых последовательностей, как предлагает следующая теорема.

Теорема 14.30. Апериодические коэффициенты корреляции λ_k, связанные с кронекеровской суммой фазовых последовательностей

$$x_1+y_1,\ x_1+y_2, \ldots,\ x_1+y_m,\ x_2+y_1,\ x_2+y_2, \ldots, x_l+y_m,$$

определяются с помощью апериодических коэффициентов корреляции $\lambda_k(x)$ и $\lambda_h(y)$ двух суммируемых последовательностей $\{x_\mu\}$, $\mu=1, 2, \ldots, l$ и $\{y_\nu\}$, $\nu=1, 2, \ldots, m$:

$$\lambda_k=\lambda_j(x)\,\lambda_h(y)+\lambda_{j+1}(x)\,\lambda^*_{m-h}(y), \quad k=jm+h,\ 0\leqslant h<m.$$

Доказательство. Пусть $\alpha_\nu=e^{(2\pi i/r)x_\nu}$ и $\beta_\nu=e^{(2\pi i/r)y_\nu}$. Тогда при $k=jm+h$, $0\leqslant h<m$, имеем

$$\lambda_k=\sum_{\mu=1}^{l-j}\sum_{\nu=1}^{m-h}\alpha_\mu\beta_\nu(\alpha_{\mu+j}\,\beta_{\nu+h})^*+$$
$$+\sum_{\mu=1}^{l-(j+1)}\sum_{\nu=m-h+1}^{m}\alpha_\mu\beta_\nu(\alpha_{\mu+j+1}\beta_{\nu-(m-h)})^*=\sum_{\mu=1}^{l-j}\alpha_\mu\,\alpha^*_{\mu+j}\sum_{\nu=1}^{m-h}\beta_\nu\,\beta^*_{\nu+h}+$$
$$+\sum_{\mu=1}^{l-(j+1)}\alpha_\mu\,\alpha^*_{\mu+j+1}\sum_{\nu'=1}^{h}\beta^*_{\nu'}\,\beta_{\nu'+m-h}=\lambda_j(x)\,\lambda_h(y)+\lambda_{j+1}(x)\,\lambda^*_{m-h}(y), \tag{14.57}$$

что и требовалось доказать ■.

Заметим, что результаты не обязательно остаются теми же в случае, когда две последовательности в кронекеровской сумме меняются местами. Заметим также, что максимальное значение нормированных апериодических коэффициентов корреляции λ_k/n нельзя снизить, используя эту конструкцию.

14.16. Синхронизация слов и кадров. Выбор статистик

В предыдущих параграфах этой главы и в гл. 11 и 12 были исследованы различные методы установления синхронизации слов. Рассмотренные методы можно разделить на две категории[1]:

1. В поток данных периодически помещается специальная син-

---

[1] Третий метод, в равной мере применимый к синхронизации слов, выборок сообщения или символов, использует дополнительный синхронизационный канал (или, что эквивалентно, использует канал связи в двух различных режимах, режиме синхронизации и режиме передачи данных). Этот подход подробно изучен в гл. 6 и здесь не будет рассматриваться. *(Прим. авт.)*.

хронизирующая последовательность (или префикс, или запятая). Опознание ее приемником устанавливает требуемую синхронизацию. Для удобства методы, относящиеся к этой категории, будем называть *префиксными методами*.

2. Используется различие между правильными словами и стыками слов для того, чтобы различить эти две ситуации. Хотя при этом подходе не обязательно используются словари без запятой (см. гл. 7), наибольший эффект получается, когда словари свободны от запятой, и поэтому метод будет называться *методом свободы от запятой*.

Следует подчеркнуть эквивалентность с более общих позиций синхронизации слов и выборок сообщения. Заменяя «слово» на «символ» и «выборку сообщения» на «слово», с равным успехом можно использовать все методы синхронизации слов для синхронизации выборок сообщения. Если каждое слово содержит k q-ичных информационных символов, то кадр может быть рассмотрен как слово, составленное из q^k-ичных символов. Относительная привлекательность различных подходов, конечно, может изменяться, когда рассматривается синхронизация выборок сообщения, а не синхронизация слов, но существенная эквивалентность этих двух задач будет оставаться неизменной.

В следующем параграфе будет оценена синхронизационная задержка, свойственная как префиксному методу, так и методу свободы от запятой. Под синхронизационной задержкой здесь подразумевается число слов или символов, необходимых для первоначального входа в синхронизм с заранее заданной надежностью. Следует отметить отличие этого определения синхронизационной задержки и того, которое было использовано в гл. 11 в ситуации, когда отсутствовал шум. Родственная задача возвращения в синхронизм после его потери отличается от задачи первоначального входа в синхронизм только изменением априорных вероятностей различных конкурирующих синхронизационных позиций и отдельно не будет здесь рассматриваться.

Однако до того, как приступить к этой задаче, нужно выбрать статистику, на основе которой будет принято решение относительно того, была или не была достигнута синхронизация. С этой целью представим сигнал дискретным множеством наблюдаемых $Y=\{y_i\}$. (В случае гауссовского канала эти y_i могут быть выборками принимаемого сигнала, взятыми через равные интервалы времени; если канал является уже дискретным, как в случае q-ичного симметричного канала, то эти величины являются символами на выходе приемника.) Так же, как и при рассмотрении символьной синхронизации, удобно разделить полный период неоднозначности T на конечное число N меток ν, $\nu=0, 1, 2, \ldots, N-1$, где $N=T/\Delta t$. Обычно в предположении, что синхронизация более низкого порядка уже была установлена, это квантование по времени является весьма естественным.

Рассмотрим вначале ситуацию, когда в информационный поток периодически помещается синхронизирующая последовательность или префикс. Разделим множество выборок y_i на два подмножества Y_1 и Y_2, где $Y_1 = Y_1(\nu)$ содержит те выборки y_i, которые берутся из префиксной части принимаемого сигнала в предположении, что ν-я метка является верной, а $Y_2 = Y_2(\nu)$ — множество, остающееся после того, как Y_1 будет удалено из Y. Обозначая через $p(A|B)$ вероятность (или плотность вероятности) события A при условии события B и предполагая, что шум действует на последовательные выборки независимо, получим

$$p(Y \mid \nu) = \sum_{D} p(Y_2 \mid D, \nu)\, p(D)\, p(Y_1 \mid S, \nu). \tag{14.58}$$

Каждое из множеств D является множеством информационных выборок, которые наблюдались бы в отсутствие шума с вероятностью $P(D)$. Аналогично S является множеством выборок, характеризующих префикс в отсутствие шума. Оптимальное решение (максимального правдоподобия) состоит в выборе такой метки ν, для которой максимальна вероятность $P(Y|\nu)$. (Это соответствует случаю, когда одно и то же множество наблюдаемых Y используется для проверки всех меток, т. е. случаю параллельного поиска. Однако, как и в гл. 6, будем использовать одно и то же правило решения как для параллельного, так и для поочередного поиска.)

Суммирование по D в ф-ле (14.58) весьма неудобно с практической точки зрения и хотелось бы иметь возможность приравнять эту сумму постоянной, не зависящей от ν. К сожалению, эта строгая независимость наблюдается крайне редко. Если информационная последовательность состоит из независимых символов и все последовательности равной длины равновероятны, и если выборки y_i берутся после того, как выносятся жесткие решения относительно каждого принятого символа, то сумма на самом деле, не зависит от ν. Однако в более общей ситуации этот случай не имеет места. Кроме случая, когда жесткие решения уже были сделаны, шум неизбежно будет приводить к тому, что некоторые множества выборок $Y_2(\nu)$ будут напоминать информационную последовательность более сильно, чем другие. То же самое утверждение справедливо, когда на информационную последовательность наложены какие-либо ограничения, например, когда она закодирована с целью защиты от ошибок или с целью не допустить появления синхронизирующей последовательности.

Тем не менее вследствие того, что с точки зрения реализации получающийся синхронизатор имеет практические преимущества и в силу того, что упрощенный синхронизатор более удобен для анализа, не будем учитывать суммирование по информационной последовательности в (14.58). Следует, однако, признать, что получающийся синхронизатор, использующий теперь единственную решающую переменную

$$z_\nu = p(Y_1 \mid S, \nu), \tag{14.59}$$

в общем случае является подоптимальным.

Для канала с белым гауссовским шумом решающая переменная z_ν после отбрасывания выражений, которые не зависят от ν, и перехода к пределу, когда частота выборок стремится к бесконечности, принимает вид

$$z_\nu = \sum_j \int\limits_{j T_r + \nu\Delta t}^{j T_r + T_s + \nu\Delta t} y(t)\, s(t - \nu\,\Delta\, t)\, dt. \qquad (14.60)$$

Здесь T_r — временной интервал между последовательными появлениями префикса; T_s — длительность префикса; $y(t)$ — принимаемый сигнал и $s(t)$ префиксный сигнал [причем $s(t + iT_r) = s(t)$ при всех i].

Решающая переменная для q-ичного симметричного канала также легко может быть найдена. Если расстояние Хэмминга между j-м повторением предполагаемого префикса в множестве выборок $Y_1(\nu)$ и действительным префиксом, представляемым множеством S, равно $n_j(\nu)$ и если $\sum_{j=1}^{M} n_j(\nu)\, d_\nu$, то $z_\nu = p^{d_\nu}(1-p)^{Mn-d_\nu}$, где p — вероятность ошибки в символе; n — число символов в синхронизирующей последовательности, а M — число повторений префикса, используемых для решения. Если $p < 1/2$, то метка, выбранная с помощью критерия максимального правдоподобия, минимизирует сумму

$$d_\nu = \sum_j n_j(\nu). \qquad (14.61)$$

Для упомянутого выше второго метода синхронизации, метода свободы от запятой, вероятность $p(Y|\nu)$ обычно выражается в виде

$$p(Y \mid \nu) = \sum_D p(Y \mid D, \nu)\, P(D), \qquad (14.62)$$

где обозначения те же самые, что и в (14.58). Так как при этом отсутствует синхронизирующая последовательность, то вся информация теперь содержится в сумме по D. В силу того что мы интересуемся применением этого метода, когда информация кодируется с помощью словаря без запятой, будем предполагать, что информация представляется последовательностью слов, каждое из которых выбирается случайно из словаря, содержащего N слов w_i, $i = 1, 2, \ldots, N$. Тогда, разделив Y на непересекающиеся подмножества $Y_j = Y_j(\nu)$, соответствующие интервалу, на котором принимается j-е слово при условии, что правильной является ν-метка, будем иметь

$$p(Y \mid \nu) = \frac{1}{N} \prod_j \sum_i p(Y_j \mid w_i, \nu). \qquad (14.63)$$

Это, конечно, равносильно ситуации, с которой мы сталкивались при исследовании методов символьной синхронизации (см. гл. 7).

В случае синхронизации слов в особенности справедливо то, что одно из слагаемых $p(Y_j|w_i, \nu)$, по-видимому, будет значительно больше, чем остальные, когда ν в действительности является правильной меткой. (Если это не так, вероятность ошибки при синхронизации слов, вообще говоря, будет неприемлемо высокой.) Следовательно, если правильной является ν-я метка, то имеем

$$p(Y|\nu) \approx \frac{1}{N} \prod_j \max_i p(Y_j | w_i, \nu). \tag{14.64}$$

Решение максимального правдоподобия состоит в выборе той метки, для которой вероятность $p(Y|\nu)$ достигает максимума. Так как $p(Y|\mu)$ можно хорошо аппроксимировать выражением (14.64), когда μ является правильной меткой, и так как

$$p(Y|\nu) \geqslant \frac{1}{N} \prod_j \max_i p(Y_j | w_i, \nu)$$

для любой метки ν (все отброшенные слагаемые неотрицательны), то решение не должно быть значительно менее надежным в случае, если оно основывается на приближении (14.64), а не на точном выражении (14.63). Преимущества использования этого приближения очевидны. (Между прочим, та же самая решающая переменная получится, если производится совместное решение максимального правдоподобия относительно как принимаемой последовательности слов $\{w_i\}$, так и метки ν.)

Для канала с белым гауссовским шумом решающая переменная, которая получается после того, как берется логарифм (14.64) и отбрасываются выражения, не зависящие от ν, имеет вид

$$z_\nu = \sum_i \max_j \int\limits_{iT_w+\nu\Delta T}^{(i+1)T_w+\nu\Delta t} \left[y(t)\, w_j(t-\nu\Delta t) - \frac{1}{2} w_j^2 (t-\nu\Delta T) \right] dt, \tag{14.65}$$

где T_w — длительность слова[1]. Синхронизатор выбирает μ-ю метку, если $z_\mu > z_\nu$ при всех $\nu \neq \mu$.

Решающая переменная для q-ичного симметричного канала, которая получается из приближения (14.64), имеет вид

$$d_\nu = \sum_i \min_j n_i(j; \nu), \tag{14.66}$$

где $n_i(j; \nu)$ — хэмминговское расстояние между принимаемой на i-м интервале последовательностью и j-м словом кодового словаря. При этом синхронизатор выбирает μ-ю метку, если $d_\mu < d_\nu$ при всех $\nu \neq \mu$.

---

[1] Это не что иное, как решающая переменная фазовокогерентного синхронизатора. Обобщение на фазовонекогерентный случай аналогично во всех существенных моментах соответствующему обобщению в гл. 7. (*Прим. авт.*).

14.17. Синхронизация слов и кадров. Синхронизационная задержка

Несмотря на то, что в некоторых частных случаях относительно просто получить точные ответы, здесь рассмотрим лишь один метод приближенного определения задержки, необходимой для получения синхронизации слов или кадров. Оправдание этого подхода состоит в общности и интерпретируемости результатов, а также в том, что более точные оценки можно получить (если это вообще возможно) только за счет значительного усложнения анализа. Это приближение использует, во-первых, границу

$$P_0 \leqslant P_e \leqslant (N-1) P_0 \tag{14.67}$$

для вероятности ошибочного решения о синхронизации, где

$$P_0 = \begin{cases} \max\limits_{\nu \neq \mu} \Pr\{ z_\mu < z_\nu \}, & \text{гауссовский канал;} \\ \max\limits_{\nu \neq \mu} \Pr\{ d_\mu > d_\nu \}, & q\text{-ичный симметричный канал,} \end{cases}$$

а μ обозначает правильную метку. Для удобства и без потери общности в последующем рассмотрении положим $\mu=0$. Далее заметим, что статистики z_0, z_ν, d_0 и d_ν обычно являются суммами большого числа независимых случайных величин и можно применить центральную предельную теорему к разности

$$y_\nu = \begin{cases} z_0 - z_\nu, & \text{гауссовский канал;} \\ d_\nu - d_0, & q\text{-ичный симметричный канал.} \end{cases} \tag{14.68}$$

При этом так же, как и в гл. 6 и 7, для оценки синхронизационной задержки можно использовать решение уравнения

$$r^2 \triangleq \min_{\nu \neq 0} \frac{E^2(y_\nu)}{\operatorname{var}(y_\nu)} = 2 k_N \log_e \frac{1}{P_e}. \tag{14.69}$$

Напомним, что постоянная k_N ограничена неравенством $1 \leqslant k_N \leqslant 1+[\log_e(N-1)/\log_e(1-P_e)]$, так что в большинстве случаев $k_N \approx 1$.

Этот метод оценивания синхронизационной задержки хорош либо когда наблюдения, относящиеся к различным меткам, производятся одновременно, либо когда они производятся поочередно в соединении с поиском с фиксированным объемом выборки (см. гл. 6). Хотя этот вопрос и не исследуется здесь, алгоритм последовательного поиска, по-видимому, также можно было бы использовать с целью получить некоторое преимущество при определении меток слов или кадров. Однако, так как наблюдаемые в общем случае подчиняются довольно причудливым распределениям, обычно осуществляется аппроксимация оптимального теста.

Рассмотрим теперь некоторые частные примеры.

Префиксный метод; q-ичный симметричный канал. Если можно предполагать, что информационные символы взаимно независимы и имеют равномерное распределение, то когда $\nu \geqslant m$ (где m обозначает число символов в префиксе) и когда до вынесения решения производится M наблюдений, то

$$\left.\begin{aligned} &E(d_0) = Mmp; \quad E(d_\nu) = Mm(q-1)/q; \\ &\operatorname{var}(d_\nu - d_0) = \operatorname{var}(d_\nu) + \operatorname{var}(d_0) = Mm\left[p(1-p) + \frac{q-1}{q^2}\right], \end{aligned}\right\} \tag{14.70}$$

где p — вероятность ошибки в символе. Предполагается, что префикс выбирается так, чтобы метки $\nu < m$ были более легко отличимы от правильной метки по сравнению со случаем $\nu \geqslant m$. В действительности последовательности баркеровского типа удовлетворяют ограничениям, обеспечивающим как раз это свойство. Из (14.69) при этом получаем

$$M = \frac{p(1-p) + (q-1)/q^2}{m(1 - 1/q - p)^2}\, 2k_N \log_e \frac{1}{P_e}. \tag{14.71}$$

Это и есть приближенное число наблюдений префикса, необходимое для того, чтобы достичь вероятности ошибки P_e (в случае, когда все метки наблюдаются одновременно). Конечно, поочередное наблюдение будет продолжаться в N раз дольше.

Возникает вопрос относительно преимущества запрещения префиксу появляться в случайном потоке данных, что могло бы быть выполнено с помощью использования либо префиксных кодов, либо кодов с запятой. Преимущество довольно очевидно, когда вероятность ошибки очень мала и необходимы лишь несколько наблюдений для того, чтобы вынести надежное решение. В противоположность этому, когда вероятность ошибки в символе имеет достаточно большую величину, то требуется относительно большое число наблюдений [и тем самым справедливы приближения, приводящие к ф-ле (14.71)] и эти преимущества исчезают. Единственным влиянием этих ограничений на последовательность данных является небольшое увеличение $E(d_\nu)$ и некоторое уменьшение $\operatorname{var}(d_\nu)$. Ни одно из этих изменений не меняет существенно результат (14.71). Тот же самый вывод несправедлив, однако, при условии, что информационная часть принимаемого сигнала не опускается при определении решающей переменной [см. (14.58) и следующее за ним обсуждение]. В этом случае процедура синхронизации будет принадлежать к классу методов свободы от запятой, а не к префиксному классу в смысле терминов, введенных выше).

Префиксный метод-канал с белым гауссовским шумом. Если сигнал, переносящий информацию $x(t)$, статистически ортогонален к префиксу $s(t)$ и если $s(t)$ имеет единичную среднюю мощность, то

$$E(z_0) = MAT_s; \quad E(z_\nu \mid \nu\Delta T > T_s) = 0;$$

$$\operatorname{var}(z_0) = MN_0T_s/2;$$

$$\operatorname{var}(z_\nu \mid \nu\Delta T > T_s) = MN_0T_s/2 + MA^2T_s^2\sigma_0^2.$$

где

$$\sigma_0^2 = E\left\{\left[\frac{1}{T_s}\int\limits_0^{T_s} x(t+\nu\Delta T)\, s(t)\, dt)\right]^2 \middle| \nu\Delta T > T_s\right\}, \tag{14.72}$$

а N_0 — односторонняя спектральная плотность шума. Тогда, положив $R_s = A^2 T_s/N_0$, находим, что требуемое число повторений префикса приближенно равно

$$M = [(1 + R_s\sigma_0^2)/R_s]\, 2k_N \log_e(1/P_e). \tag{14.73}$$

В еще более частном случае как префикс, так и информация представляются последовательностями двоичных символов вида $\pm\sqrt{2}\sin\omega t$, где каждый символ имеет длительность T_s/m секунд. Тогда, если последовательные информационные символы взаимно независимы и равномерно распределены, то

$$\sigma_0^2 = \frac{1}{2^m}\sum_{l=0}^{m}\binom{m}{l}\left(1 - \frac{2l}{m}\right)^2 = \frac{1}{m}. \tag{14.74}$$

Метод свободы от запятой; q-ичный симметричный канал; коды, исправляющие ошибки. В общем случае трудно оценить синхронизационную задержку в случае отсутствия запятой без детального рассмотрения конкретного используемого словаря. Трудность появляется потому, что теперь решение основывается не на расстояниях между принимаемыми n-последовательностями при некоторой заданной метке и известным префиксом, а на расстоянии между этими n-последовательностями и ближайшими к ним кодовыми словами. Имеются фактически q^k префиксов вместо одного.

Предположим, что расстояние между принимаемым стыком слов и ближайшим кодовым словом (пусть w_i) в отсутствие ошибок равно δ. Математическое ожидание расстояния между этой n-последовательностью и w_i равно

$$(n-\delta)p + \delta\left(1 - \frac{p}{q-1}\right) = np + \delta\left(1 - \frac{q}{q-1}p\right), \tag{14.75}$$

когда вероятность ошибки в символе равна p.

К сожалению, это верхняя граница для математического ожидания расстояния между принимаемой n-последовательностью и ближайшим кодовым словом, так как ближайшее кодовое слово после того, как произошли ошибки, может уже не быть словом w_i.

Несмотря на это, если рассматриваемый словарь имеет минимальное расстояние d и индекс свободы от запятой s, если s мало по сравнению с $d/2$ и если вероятность ошибки в слове (при наличии синхронизации) мала, то граница (14.75) (где $\delta = s$) дает разумную оценку для математического ожидания минимального расстояния между стыком слов и словом. Если стык слов в действительности отличается лишь s символами от любого кодового слова, то (14.75) ограничивает сверху математическое ожидание минимального расстояния, как уже было отмечено. Но если произошло менее чем $(d/2)-s$ ошибок, то первоначально ближайшее слово будет и далее оставаться ближайшим словом, а так как вероятность $(d/2)-s$ или большего числа ошибок должна быть малой при указанных предположениях, то этот эффект, по-видимому, будет сравнительно малым. Более того, хотя гарантируется, что минимальное расстояние в отсутствие ошибок равно s, в наиболее общем случае оно будет превышать s, и так как математическое ожидание расстояния (14.75) является возрастающей функцией δ, то оценка, полученная приравниванием δ к s, является в этом смысле консервативной.

Для оценки синхронизационной задержки положим

$$\left.\begin{aligned} &E(d_0)=Mnp;\\ &E(d_\nu)=Mnp+Ms\left(1-\frac{q}{q-1}p\right);\\ &\operatorname{var}(d_0)=\operatorname{var}(d_\nu)=Mnp(1-p).\end{aligned}\right\} \tag{14.76}$$

Дисперсии, приведенные здесь, являются дисперсиями расстояния между рассматриваемой n-последовательностью и ближайшим словом при отсутствии ошибок; следовательно, они являются верхними границами для действительных дисперсий величин d_0 и d_ν. Заметим, что d_0 и d_ν не являются независимыми в случае, если эти две метки наблюдаются одновременно. Тем не менее, так как для любых двух случайных величин x и y

$$\begin{aligned} E(x-y)^2 &= E(x^2)+E(y^2)-2E(xy)\leqslant E(x^2)+E(y^2)+\\ &+2E^{1/2}(x^2)E^{1/2}(y^2)=[E^{1/2}(x^2)+E^{1/2}(y^2)]^2,\end{aligned} \tag{14.77}$$

то получаем

$$\operatorname{var}(y_\nu)\leqslant\begin{cases}2Mnp(1-p), & \text{поочередное наблюдение;}\\ 4Mnp(1-p), & \text{параллельное наблюдение.}\end{cases}$$

В соответствии с этим находим приближенную оценку общего числа кодовых слов, которые должны быть приняты для того, чтобы гарантировать надежное решение:

$$M=\begin{cases}\dfrac{2p(1-p)}{\left[\dfrac{s}{n}\left(1-\dfrac{q}{q-1}p\right)\right]^2}\,2k_n\log_e\dfrac{1}{P_e}, & \text{поочередное наблюдение;}\\[2ex] \dfrac{4p(1-p)}{n\left[\dfrac{s}{n}\left(1-\dfrac{q}{q-1}p\right)\right]^2}\,2k_n\log_e\dfrac{1}{P_e}, & \text{параллельное наблюдение}.\end{cases} \tag{14.78}$$

Следует подчеркнуть, что эти результаты дают лишь оценку синхронизационной задержки; они не являются ни границей снизу, ни границей сверху для этой задержки.

Метод свободы от запятой; канал с белым гауссовским шумом; ортогональные коды. Если D —

ортогональный $(n=r^k,\ k)$-словарь с максимальным асинхронным коэффициентом корреляции ρ_m, то можно доказать, что

$$\left.\begin{aligned} &E(z_0) \approx MAT_w; \\ &E(z_\nu) \leqslant MAT_w \rho_m + M(N_0 T_w/2)^{1/2}\sqrt{2\log_e n} + O\left(1/\sqrt{\log_e n}\right) \end{aligned}\right\}. \tag{14.79}$$

Так как все слова имеют равную мощность $P_w=A^2$, то второе слагаемое под знаком интеграла, определяющего z_ν [см. (14.65)], здесь было опущено. Величина T_w — длительность слова, а N_0 — односторонняя спектральная плотность шума. Аналогично

$$\operatorname{var}(z_0) = MN_0 T_w/2; \quad \operatorname{var}(z_\nu) \approx M\pi^2 N_0 T_w/24 \log_e n. \tag{14.80}$$

В соответствии с этим из ф-лы (14.69) получаем

$$M \approx \begin{cases} \dfrac{n(1+\pi^2/12\log_e n)\,2k_n \log_e(1/P_e)}{2R_b(\log_2 n)\,[(1-\rho_m)-(\log_e 2/R_b)^{1/2}]^2}, & \text{поочередное наблюдение;} \\ \dfrac{(1+\pi/\sqrt{12\log_e n})^2\,2k_n \log_e(1/P_e)}{2R_b(\log_2 n)\,[(1-\rho_m)-(\log_e 2/R_b)^{1/2}]^2}, & \text{параллельное наблюдение,} \end{cases} \tag{14.81}$$

где $R_b=A^2T_w/N_0\log_2 n$ — отношение энергии сигнала на бит к спектральной плотности шума. Очевидно, что достаточным для синхронизируемости ортогональных кодов является условие

$$R_b > \log_e 2/(1-\rho_m)^2. \tag{14.82}$$

Вероятность ошибки в слове при использовании ортогонального множества сигналов была найдена в § 4.2, она стремится к нулю асимптотически с ростом числа слов n только если $R_b > \log_e 2$. Так как, по-видимому, ρ_m должно стремиться к нулю при $n \to \infty$ (хотя это и не было доказано, то условие для синхронизируемости ортогональных кодов, по крайней мере, асимптотически совпадает с условием малости вероятности ошибки в слове.

Тем не менее условие (14.82) дает чрезвычайно консервативную оценку отношения сигнал/шум, требуемого для синхронизации. Одной из главных причин этого является предположение, которое неявно присутствует в (14.79), что любой стык слов имеет максимально возможную корреляцию с каждым кодовым словом. За исключением, возможно, очень больших ортогональных словарей, такое предположение делает несправедливым утверждение теоремы 14.29. Большинство стыков слов не будут коррелированы так сильно с каким-либо словом словаря и, конечно, не будут коррелированы так одновременно со всеми словами. Значительно более точные оценки синхронизационной задержки, связанные с ортогональными кодами без запятой, были получены при использовании ограничения, приведенного в теореме 14.29. Однако даже эти границы остаются весьма консервативными. Экспериментальные данные показывают, что в типичном случае требуется лишь несколько (5—10) принятых слов для того, чтобы вынести решение относительно какой-либо частной метки с приемлемо малой вероятностью ошибки.

АЛФАВИТНО-ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ

Абсолютно самосинхронизирующиеся коды 303
, универсальная синхронизирующая последовательность 309—311
, условия 304—309
Аддитивная граница для вероятности ошибки 44, 86
Аддитивно-циклическое свойство 373
АИМ 61—69 (см. также Амплитудно-импульсная модуляция)
Алгебраически синхронизируемые коды, исправляющие ошибки 447—451
Алгебраическое декодирование 395—398
Алфавит
источника 284
канала 284
символов 77
Альтернативная гипотеза 14
Амплитудно-импульсная модуляция
, влияние несовершенной синхронизации 263—273
, символьная синхронизация 200—207, 217—226, 226—231
, системы ФАПЧ 234—238
, оптимальное распределение мощности 273—279
фазовокогерентная 61—64
фазовонекогерентная 64—69
Апериодический коэффициент корреляции 462
Асимптотически эффективная оценка 47
Асинхронный коэффициент корреляции 458—461
, границы 458—461
кронекеровского произведения кодов 459—461

Байесовская оценка 46
Байесовский тест 15, 43
Баркера последовательности 427—432
обобщения 430—432
Баркера фазовые последовательности 461—463
Белый шум 8
Биортогональный код 412
Биортогональный символьный алфавит 84—85
Блоковые коды 286, 326
, их синхронизируемость 326—354
Боуза—Чоудхури—Хоквингема коды 374—376 (см. также БЧХ коды)
БЧХ коды 374—376
их смежные классы, неуязвимые при потере синхронизации 438—439, 441

Вандермонда определитель 370
Вероятностное декодирование 398—399
Вероятность ошибки в символе 77, 91, 105—106 (см. также Вероятность ошибки на бит, Вероятность ошибки в слове)
, биортогональные символы 84—85
, границы
, когерентный прием 85—87
, некогерентный прием 93
, ортогональные символы
, когерентный прием 81—82
, некогерентный прием 92
, при несовершенной синхронизации 270—273
, равнокоррелированые символы
, когерентный прием 81—82
, некогерентный прием 92
, трансортогональные символы 84
, ФТ
, когерентный прием 97—100
, относительно когерентный прием 102—104
, при несовершенной синхронизации 263—270
Вероятность ошибки в слове (см. также Вероятность ошибки на бит, Вероятность ошибки в символе)
, граница 402—404
, связь с минимальным расстоянием 403—404
, сравнение с вероятностью ошибки в символе 105—109
Вероятность ошибки на бит 105—109 (см. также Вероятность ошибки в символе, Вероятность ошибки в слове)
для двоичной ФТ
при несовершенной символьной синхронизации 264—267
при несовершенной синхронизации несущей 263—266
при опорной несущей, получаемой с помощью системы Костаса 280—281
при оптимальном распределении мощности 276
Вероятность ошибочного декодирования 401—406
, граница 402—404
Вес вектора 359

ВИМ (см. Время-импульсная манипуляция)
Винера фильтр 111—120
Винера—Хопфа уравнение 114
Влияние неточной синхронизации 258—273, 282—283
  , АИМ 261—263
  , двоичная ФТ 263—270, 282—283
  , ортогональные символы 270—273
  , ФТ 263—270
Время входа в синхронизм (см. также Синхронизационная задержка)
  для систем ФАПЧ 136—141
  для последовательностей, быстро входящих в синхронизм 185
  , единый канал 203—204, 209, 213
  , отдельный канал 155—163, 167—168, 173
Время-импульсная манипуляция 96, 97
  , символьная синхронизация 215—217, 224—226
Выборок сообщения синхронизация 11, 463—472 (см. также Слов синхронизация)
Вырожденный класс эквивалентности 312
  в смысле ФТ 350
Высокого порядка синхронизация 9, 154—192
Генератор, управляемый напряжением 125
Гильберта граница 365, 385—386
Гипотеза
  альтернативная 14
  нулевая 14
Грайсмера граница 364
Границы (см. также Вероятность ошибки в символе, Вероятность ошибки в слове, границы для них)
  , аддитивная 44, 86
  вероятности ошибочного декодирования 402—404
  задержки декодирования 296
  индекса неуязвимости 434, 435—437
  индекса свободы от запятой 432—434
  максимального коэффициента корреляции в фазовых кодах 408
  минимального начального расстояния в сверточных кодах 385—387
  минимального расстояния в кодах, исправляющих ошибки 360—366
  минимального расстояния в кодах, исправляющих ошибки синхронизации 444
  синхронизационной задержки 301, 302, 321
  синхронизационной ошибки отслеживания 131, 164
  точности оценивания 47
  Чернова 404
  числа слов в синхронизируемых словарях 312—318, 327
  числа слов в словарях, синхронизируемых при использовании ФТ 351

Групповой код
  , фазовый код 407
Грэя код 107
ГУН 125

Двоичная ФТ 100, 104
  , влияние несовершенной синхронизации 264—267
  , оптимальное распределение мощности 274—277
  , символьная синхронизация 208—209, 222—224
  , синхронизация несущей 240—241

Декодеры (см. также Декодирование)
  источника 8
  канала 8

Декодирование 393—401, 412—413
  алгебраическое 395—398
  вероятностное 398—399
  максимального правдоподобия 393—395

  , отказ при декодировании 405
  ошибок и стираний 396
  по обобщенному максимальному расстоянию 397
    , граница для вероятности ошибки 402—404
  пороговое 399—401
  последовательное 398—399
  сверточных кодов 398—401
  с обратной связью 384
  фазовых кодов 412—413

Декодируемые коды 286
  , проверка декодируемости 293—296

Дельта-модуляция 284

Демодулятор 8, 56—61 (см. также Приемники, Устройство оценивания)
  , АИМ
    когерентный 61—64
    некогерентный 64—69
  корреляционный 59—60
  максимальной апостериорной вероятности 58
  максимального правдоподобия 58—59

  с минимальной среднеквадратической ошибкой 57
  с согласованными фильтрами 59—60
  ФТ 69—72
Детектор огибающей 89
Детерминированные сигналы 117
Дискретные системы связи 8, 76—110
Длина пачки ошибок 406
Достаточная статистика 13

Задержка декодирования 287
  , граница 296
  , условие ограниченной задержки 296
Запятая 344

Идеальный наблюдатель 16
ИКМ 284
Импульсно-кодовая модуляция 284
Импульсные системы связи
  дискретные по амплитуде 8, 51—75
  непрерывные по амплитуде 8, 51—75
Инвариантные пути
  , избыточность 353—354
  , коды без запятой с инвариантными путями 331—336
Индекс неуязвимости на *m*-й позиции 434
  БЧХ кодов 438—439
  , границы 435—437
  кодов, исправляющих пачки ошибок 451—454
  кронекеровского произведения, кронекеровской суммы и каскадных кодов 454—457
  , проверка 434
  Рида—Соломона кодов 438
  циклических кодов 437—442
Индекс неуязвимости степени 434
  , границы для него 434
Индекс свободы от запятой 432
Информационный символ 356
Источника кодер 7
Источника кодирование 284—287
  , декодируемые коды 284—296
    , проверка декодируемости 293—296
  , синхронизируемые блоковые коды 326—331
    без запятой 326—331
    без запятой с инвариантными путями 331—336
    префиксные 336—344
    при использовании ФТ 349—353
    с запятой 344—349
  , синхронизируемые коды 297—325
    , граница для числа слов в них 312—318
    , построение максимальных словарей 318—326
    , проверка синхронизируемости 297—302
    самосинхронизирующиеся 302—312
Хаффмана коды 290—293
Источник информации 7

Кадр (данные, сообщение) 11
Канал 7
  с белым гауссовским шумом 8
  многолучевой 110
  симметричный 406
Каскадные коды 381—383
  , индекс свободы от запятой 454—458
Квадратичная система 251
Квантованная ФТ 97—100 (см. также Фазовая манипуляция)
Классы векторов в порождающей матрице 377
Класс верности 392
Класс эквивалентности
  в смысле ФТ 350
  вырожденный 312
  n-последовательностей 312
  символов 315
  слов 315
  ФТ вырожденный 350
Когерентная система 70 (см. также Фазово-когерентные системы)
Код (см. также Словарь, Декодируемые коды, Синхронизируемые коды, Коды с запятой, Коды без запятой, Коды, исправляющие ошибки, Фазовые коды, Префиксные коды)
  Грэя 107
  Манчестера 227
  Хаффмана 290—293
Кодер (см. также Кодирование)
  источника 7
  канала 7
Кодирование
  линейных кодов 389
  относительное 240
  сверточных кодов 391
  фазовых кодов 412
  циклических кодов 390
Кодовое дерево 290
Кодовое ограничение в сверточных кодах 383
Кодовое слово 7, 286, 357
Кодовый символ 284
Кодовый словарь 286
Коды без запятой 326—331
  , избыточность 353—354
  , максимальное число слов 327

  , построение максимального словаря 327—328
   , доказательство свободы от запятой 328—330
  , построение кодов с четной длиной слов 330—331
  префиксные 336—344
  с инвариантными путями 331—336
  фазовые 458—461
Коды без запятой, исправляющие ошибки 418—427
Коды, восстанавливающие синхронизацию 442
Коды, исправляющие ошибки 335—413
  без запятой 418—427 (см. также Коды без запятой, иправляющие ошибки)
  , границы для минимального расстояния 360—366
  , исправление пачек ошибок 405—406
  итеративные 381
  канонические 360
  каскадные 381—383
  , кронекеровское произведение 380
  , кронекеровская сумма 380
  линейные 358—360
  , проверка 355—356
  Рида—Маллера 383
  , связь между расстоянием и возможностью исправлять и обнаруживать ошибки 357—358
  с запятой 418
  синхронизируемые 414—472 (см. также Синхронизируемые коды, исправляющие ошибки)
  систематические 360
  Хэмминга 379
  циклические 366—376 (см. также Циклические коды, исправляющие ошибки)
Коды, исправляющие пачки ошибок 405—406
  , синхронизируемость 451
Коды, исправляющие ошибки в синхронизации 442—447
Коды, обнаруживающие ошибки 355, 356, 405 (см. также Коды, исправляющие ошибки)
Коды с запятой 344—349
  , избыточность 353—354
  , исправляющие ошибки 417—418
  , связь с кодами без запятой 348—349
  , число слов в максимальном словаре 345—348
Корневого годографа метод 146
  для определения асимптотики числа слов в префиксном коде 340
Корреляционный приемник 59—60
Косинусоидальный импульс 75, 229
Костаса система 246—251
Крафта неравенство 287—290
Кронекеровская сумма кодов 380—381, 395
  , индекс свободы от запятой 454—457
Кронекеровское произведние (сумма) баркеровских фазовых последовательностей 463
Кронекеровское произведение кодов 380, 409—410
  , асинхронные коэффициенты корреляции 460—461
  , индекс свободы от запятой 454—458
Лидер смежного класса 394
Ли метрика 407
Линейная модель системы ФАПЧ 126—129
Линейные коды 358—360 (см. также Сверточные коды, Циклические коды, исправляющие ошибки)
  , кодирование и декодирование 389—401
  , неуязвимость по отношению к потере синхронизации 418—422
  порождающие 358
  , проверочная матрица 359
  Рида—Маллера 383
  сверточные 383—389
  , связь с кодами с проверками 360
  систематические 360
  Хэмминга 379
Максимального правдоподобия декодер 393—395
Максимального правдоподобия демодулятор 58—59
  , АИМ 62
  , ФТ 70
Максимального правдоподобия оценка 47
  , асимптотическая эффективность 47
Максимального правдоподобия приемник
  биортогональных сигналов 84
  когерентный 79
  некогерентный 88—89
  ФТ
   , когерентный 98
   , относительный когерентный 100—103
Максимального правдоподобия принципа оценка 48
Максимального правдоподобия символьная синхронизация 196—200
  , АИМ 200—207, 224—226

  , непрямоугольные символы 226—231
  , ортогональные символы 211—217, 224—226
    , ВИМ 215—217, 224—226
    , ЧТ 211—216, 224—226
  , отслеживание 224—227
  ФТ 207—211, 224—226
Максимального правдоподобия синхронизация несущей 234
  , АИМ 235—238
  , большое отношение сигнал/шум 242—246
  , ФТ 238—242
Максимального правдоподобия тест различения гипотез 16
Максимальной апостериорной вероятности демодулятор 59
  , АИМ 62
  , ФТ 70
Максимальной апостериорной вероятности оценка 46
Максимальной апостериорной вероятности приемник
  когерентный 78—79
  некогерентный 88—89
  ФТ
  , некогерентный прием 98
  , относительный когерентный прием 100—103
Максимальной апостериорной вероятности тест
  , две гипотезы 16
  , много гипотез 43
Максимальной длины линейные последовательности регистра сдвига 178—181 (см. также Псевдошумовые последовательности)
Максимальной длины циклические коды 372—373
  , аддитивно-циклическое свойство 373
  , распределение весов 373—374
Максимальные синхронизируемые кодовые словари 318—325
  , граница для синхронизационной задержки 321
  , граница для числа слов
    , блоковые коды 314
    , неравномерные коды 317
  , построение 318—321
  , свойство полноты 325
  , свойство префикса 319
  , свойство свободы от запятой 326—327
Манчестера код 227
Марковский источник 285
Маркуса Q-функция 93
Матрица инцидентности для кодов без запятой 332
Маттсона-Соломона многочлены 371
Мгновенно декодируемый код 288
  , достаточное условие существования 289
  , необходимое условие существования 287—288
  , число кодов 289
Мгновенно синхронизируемый код 311
Мебиуса функция 314
Метка 154
  , обнаружение 155, 196—217
  , отслеживание 217—231, 251—255
  , оценивание 163—168, 217
  , поиск 154—163, 168—169
Метод свободы от запятой для синхронизации слов 464
Мимикрии частот ошибка 55
Минимаксная оценка 58, 75
Минимаксное решение 17
Минимально-среднеквадратическая оценка 46
Минимально-среднеквадратические линейные фильтры 111—126
Минимально-среднеквадратический демодулятор 57—58
  , АИМ 64
  , ФТ 71
Многолучевой канал 110
Модулятор 7
Модуляция с пассивной паузой 226
Мощность теста различения гипотез 14

Наблюдаемые 13
Найквиста теорема отсчетов 52—55
Начальное расстояние в сверточных кодах 385
  , границы 385—387
Начальное слово 384
Неймана—Пирсона критерий 16
Некогерентный 10 (см. также Фазово-некогерентный)
Некогерентный согласованный фильтр 89
Неоднозначность во времени 11
Неравенство Рао—Крамера 47
Несущая 7
Несущей синхронизация 10, 148—154, 234—257
  , АИМ 234—238
  , большое отношение сигнал/шум 242—246
  , квадратичная система 251
  , обратная связь от решающего устройства 242—246
  , система Костаса 246—251
  , система n-й степени 251
  , ФТ 234—238
Неточность опорной фазы, ее влияние
  , АИМ 261—263

, ортогональные символы 268—273
, ФТ 266—270
Неуязвимость при синхронизации на m-й позиции
, индекс 434 (см. также Индекс неуязвимости степени μ)
кодов Хэмминга 424—425
, проверка неуязвимости 419—422
укороченных циклических кодов 423—424
циклических кодов 422—423
Никогда самонесинхронизирующиеся коды 303
Нулевая гипотеза 14
Нуль-пространство
линейных кодов 360
циклических кодов 367—368

Обеляющий фильтр 75
Обнаружение меток 155, 196—200
Обобщенное минимальное расстояние 397
, декодирование 395—398
Обратная связь от решающего устройства 242—246
Обращенный код 294
Ограничитель в системах ФАПЧ 135—136, 146—147
Огибающей детектор 89
Оптимальное распределение мощности 273—279
, АИМ 274
, ортогональные символы 277—279
, ФТ 274—277
Оптимальные линейные фильтры 111—126
Оптимизация фильтра системы ФАПЧ 129—136
Ортогонализированные коды 400
Ортогональные коды 409
Ортогональные проверочные уравнения 400
r-ортогональные фазовые коды 412
Ортогональный символьный алфавит 81
, генерирование 95—97
Ортогональных символов вероятность ошибки 80—83, 91—92 (см. также Вероятность ошибки в символе)
Ортогональных символов синхронизация 211—217, 224—226, 273—282
Остаточная ошибка
в синхронной системе связи 264
на выходе линейного фильтра 116
Отдельный канал синхронизации 148—195
, метки
, оценивание 163—168
, поиск 154—163
, отсчеты времени
, несинусоидальные 150—154
синусоидальные 148—150
, последовательности, быстро входящие в синхронизм 181—189
, псевдошумовые последовательности 175—181
, фазовонекогерентный прием 168—175
Относительная когерентная фазовая манипуляция 100—104
, символьная синхронизация 209—210, 224
Относительное кодирование 240
Относительный когерентный прием 100
Отслеживающие фазу устройства оценивания 124—126
Отсчетов времени синхронизации 9 (см. также Несущей синхронизация)
Отсчетов теорема 52—55
ОФТ (см. Относительная когерентная фазовая манипуляция)
Оценивание
, граница точности 47
статистических параметров 45—48
Оценка [см. также Оценивание, Устройство оценивания (формула оценки)]
асимптотически эффективная 47
байесовская 46
максимального правдоподобия, 47, 58
минимаксная 58—75
минимизирующая среднеквадратическую ошибку 46, 57, 111—113
по максимуму апостериорной вероятности 46, 58
по принципу максимума правдоподобия 48
эффективная 47
Ошибка
второго рода 14
первого рода 14
Ошибок вероятности (см. также Вероятность ошибки на бит, Вероятность ошибки в символе, Вероятность ошибки в слове)
границы
для кодов, исправляющих ошибки, 402—404
при фазовокогерентном приеме 85
при фазовонекогерентном приеме 93
сравнение вероятностей ошибок на бит, в символе, в слове 105—109

Ошибок и стираний декодирование 396
Переходные ошибки в системах ФАПЧ 132
Период повторения для префикса 337
Период п-последовательности 312—313
Перфорированные циклические коды 376—379
Плоткина граница 364
Поднесущая 7, 258
Поиск 26—42, 154—163
  меток 154—163
  непрерывно продолжаемый 36
  оптимальный 39—40
  последовательный 32—40, 161, 163
  с задержанным решением 159—161
  с фиксированным объемом выборки 29—32, 156—161
Полифазные коды 407—410, 458—461 (см. также фазовые коды)
Полностью ортогонализируемые коды 400
Полный словарь 289—290, 325—326
Полуупорядоченные разбиения целого числа 316
Пополнение кодового словаря 305
Пороговое декодирование 399—401
Порождающая матрица
  , линейные коды 358
  , сверточные коды 383
  , циклические коды 368
Порождающий многочлен
  нуль-пространства циклического кода 369
  циклических кодов 367
Порождающие линейного кода 358
Последовательное декодирование 398—399
Последовательности, быстро входящие в синхронизм 181—189
Последовательный поиск 32—40, 161, 163
Последовательный тест отношения плотностей вероятностей
  , много гипотез 44—45
  , простые гипотезы 17—22
  , сложные гипотезы 25—26
Потери синхронизации вероятность 146
Правдоподобия принцип 47
Правдоподобия уравнение 47
Правдоподобия функция 16
Правильный симплекс в качестве алфавита 84
Предсказывающий фильтр 119
Префикс кодового слова 288
Префиксная процедура построения максимальных синхронизируемых кодовых словарей 319—321
  , доказательство оптимальности 322
  , доказательство синхронизируемости 320—321
  , порождающая функция для числа слов в словаре 323
Префиксные коды 336—344
  , исправляющие ошибки 415—417
  модифицированные 337
  , число слов в них 337—344
Префиксный метод синхронизации слов 464
Приемник
  максимальной апостериорной вероятности 78, 88—89
  с классами верности 392
  с согласованными фильтрами 79
    некогерентный 89
  фазовокогерентный 78—81
  фазовонекогеретный 88—91
  ФТ 98
    , относительной когерентной ФТ 100—104
Проверка 356, 359—360
  , вектор 359
  , матрица 359
  , порождающий многочлен 368
  , символ 356
Проверка гипотез (тест)
  , много гипотез 42—45
  , простые гипотезы 14—17
  , сложные гипотезы 22—26
Проверка гипотез при фиксированном объеме выборки
  много гипотез 42
  , простые гипотезы 14
  , сложные гипотезы 22
Псевдослучайные последовательности (см. Псевдошумовые последовательности)
Псевдоциклические коды 377
Псевдошумовые последовательности 175—181, 253—254, 372—381
Путь на кодовой матрице инцидентности 332
ПШ-последовательности (см. Псевдошумовые последовательности)
Равномерно наиболее мощный тест 24
Равномерные сверточные коды 388
Разбиваемый код 304
  , необходимое и достаточное условие 306, 308—309
Райсовское распределение 91

Распределение мощности в синхронных системах связи 258—283 (см. также Оптимальное распределение мощности)
Расстояние
  Ли 407
  начальное 385
  обобщенное минимальное 397
  хэмминговское 358
Расширение максимального синхронизируемого словаря 320
Расщепленный строб
  синхронизатор с расщепленным стробом 222—226
Рациональный спектр 116
Ребер синхронизация 415
Регистр сдвига, линейный с обратной связью 177, 373, 390
Релеевские замирания в канале 110
Релеевское распределение 91
Решающие переменные 155
Рида—Маллера коды 383
  , индекс свободы от запятой 457—458, 461
Рида—Соломона коды 376
  , индекс неуязвимости 440—441
  , исправляющие ошибки синхронизации, 443—444
Самосинхронизирующиеся коды 302—312
Сардинаса—Паттерсона алгоритм 293—295
Сверточные коды 383—389
  , декодирование 398—401
  , длина кодового ограничения 383
  , начальное расстояние 384—385
   , граница 385—387
  , начальное слово 384
  , порождающая матрица 383
  , скорость передачи информации 383
Свободы от запятой индекс 432—434, 441
  , граница 432—433
  кронекеровского произведения, кронекеровской суммы и каскадных кодов 454—458
   Рида—Маллера кодов 457—458, 461
Свойство префикса 288, 319
Сглаживающий фильтр 119
Сегмент суффиксного разложения 293
Сигнал/шум, отношение в импульсных системах связи 55
Символ
  данных 7
  информации 355
  источника 284
  канала 77
  кода 284, 355
  приемника 392
  проверочный 356
Символы приемника 392
Символьные синхронизаторы 196—233
  АИМ 200—207, 217—231
  максимального правдоподобия 196—200, 217
  , непрямоугольные символы 226—231
  , ортогональные символы 211—217, 224—226
  , отслеживание 217—226
  , символы, имеющие «тонкую структуру», 251—256
  с отстающим и опережающим стробированием 222—226
  ФТ 207—211, 217—231
Символьные синхронзаторы с дифференцированием 229—230
Символьный алфавит 77
Симметричный канал 406
Сингулярность запятой 344
Синдром 394—495, 425, 448
Синхронизатор с отстающим и опережающим стробированием 222—223
Синхронизаторы, отслеживающие символы 217—222
  , когерентная АИМ, бифазная ФТ 217—224
  , некогерентная АИМ, недвоичная ФТ, относительная когерентная ФТ 224
  , непрямоугольные символы 226—231
  , ортогональные символы 224—226
Синхронизационная задержка 297, 414—415
  в канале с гауссовским белым шумом
   , метод свободы от запятой 470—471
   , префиксный метод 469—470
  в каналах с шумами 468—472
  в q-ичном симметричном канале 470—471
   , метод свободы от запятой 470—471
   , префиксный метод 468—469
  , границы 301—302, 321
  для кодов без запятой 326
  для кодов без запятой с инвариантными путями 333
  , условие ограниченности задержки 298—299
Синхронизационная ошибка отслеживания
  , границы 131, 164, 192—195
  , ошибка отслеживания несущей

    , АИМ 237—238
    , большое отношение сигнал/шум 244—245
  при отдельном канале 150, 152, 153
  ФТ 242
  , ошибка отслеживания символа
    , АИМ ФТ 221, 223—224, 229—230
    , ортогональные символы 224—226
  системой Костаса 248—250
Синхронизация 9 (см. также Несущей синхронизация, Выборок сообщения синхронизация, Символ, Слово)
  в каналах с шумом 426—427
  , выбор символов для синхронизации 175—188
  высшего порядка 10, 154—192
  , границы для точности 131, 164, 192—194
  кадров сообщения 11
  несущей (отсчетов времени) 10, 148—154, 234—257
  , неуязвимость на *m*-й позиции 419—422
    , уравнение для неуязвимости 419
  по отдельному каналу 148—195
  ребер 415
  символов 10, 196—233
  слов 11
  , сравнение синхронизации по единому каналу с синхронизацией по отдельному каналу 279—282
  узлов 415
  фазовонекогерентная 168—175
Синхронизируемость 297(см. также Синхронизируемые коды)
Синхронизируемые коды 297 (см. также Коды с запятой, Коды без запятой, Префиксные коды, Синхронизируемые при использовании ФТ коды, Синхронизируемые коды, исправляющие ошибки, Синхронизируемые фазовые коды)
  блоковые 326—354
    , избыточность 353—354
    , построение 327—328, 331
  , граница для числа слов 312—318, 327
  с различными длинами слов 297—325
    , максимальное число слов длины *L* или меньше 325
      , проверка 298—299
    , построение, 318—325
Синхронизируемые коды, исправляющие ошибки 414—472
  алгебраически синхронизируемые 447—451
  , границы для расстояния 444
  , коды без запятой 418—425
  , коды, исправляющие пачки ошибок 451—454
  , коды с запятой 417—418
  , префиксные коды 415—417
  , циклические коды 437—441
Синхронизируемые при использовании ФТ коды
  , избыточность 349—353
Синхронизируемые фазовые коды 458—461
Синхронизирующие последовательности 304—305
Синхронная система связи 6
Система синхронизации с задержкой 195
Системы отслеживания при большом отношении сигнал/шум для несущей 242—246
Систематические коды 360
  , граница для индекса неуязвимости 436
  , уязвимость по отношению к потере синхронизации 423
Системы отслеживания при наличии «тонкой структуры» 251—255
Системы ФАПЧ 125—146
  , вероятность потери синхронизации 146
  , время входа в синхронизм 136—141
  второго порядка 133
    с неточным интегратором 146
  для несинусоидальных сигналов 141—146, 150—154
  , линейная модель 126
  обобщенные
    для отслеживания модулированной несущей 234—251
    для символьной синхронизации 217—231
  , оптимизация 129—136, 148—154
  , ошибка отслеживания 131—134
  первого порядка 133
  , построение сигналов 148—154
  , среднее время потери синхронизации 146
  третьего порядка 134
  , ширина полосы 131
  , эффективная амплитуда сигнала 144, 150—151, 219
Скорость передачи информации 357
  для сверточных кодов 383
Словарь
  декодируемый 286
  , исправляющий ошибки 357
  кодовый 286

  мгновенно декодируемый 288
  обращенный 294
  полный 289
Слово
  кодовое 7, 286, 357
  данных 7
Слов синхронизация 11
  , блоковые коды 326—354
  , выбор статистик 463—468
  , коды, исправляющие ошибки, 414—472
  , неравномерные коды 297—325
  , синхронизационная задержка в канале с шумами 468—472
Смежный класс фазового кода 411
Смещение статистической оценки 47
Согласованные фильтры 59
  , некогерентные 89
Состояние источника 13
Спектральная плотность мощности импульсной последовательности 56
Спектр импульсной последовательности 56
Среднее время потери синхронизма 146
Среднеквадратическая ошибка, задающая стоимостную функцию 46
Среднеквадратическая ширина полосы 193
Статистика 13
  , n-ой степени система 251
Степенная группа фазового кода 408
Стираний декодирование 396
Стирающий канал 393
Стоимостная функция 45
Стоимость статистического решения 14
Суффикса свойство 295
Суффикс кодового слова 288
Суффиксное разложение
  , кодовый словарь 293
  множества 299
Тест отношения плотностей вероятностей 17
Тест среднего максимального правдоподобия для различения гипотез 24
Тихонова распределение 147, 265
Трансортогональный код 409
Трансортогональный символьный алфавит 84
Узлов синхронизация 415
Укороченные циклические коды 376—379
  алгебраически синхронизируемые 448—449
  неуязвимые по отношению к потере синхронизации 423—424
Универсальная синхронизирующая последовательность 309—311
Упорядоченные разбиения целого числа 316
Уровень значимости теста различения гипотез 14
Устойчивый фильтр 114
Устранение избыточности в сообщении 286
Устройство автоматической регулировки усиления 135—136
Устройство оценивания (формула оценки) 46
  меток 163—168
    модулированного сигнала 217
  , минимизирующее среднеквадратическую ошибку 113—126
  фазы 69—72, 123—126, 141—146
    модулированной несущей 235—251
Фазовая манипуляция(см. также Двоичная ФТ)
  , влияние неточной синхронизации 263
  , дискретная амплитуда 97—100
  квантованная 97—100
  непрерывная по амплитуде 69—72
  , оптимальное распределение мощности 273—279
  , относительный когерентный прием 100—104
  , символьная синхронизация 207—211, 217—231
  системы отслеживания несущей 238—246
Фазовокогерентные ортогональные коды 409
Фазовокогерентные системы 10
Фазовокогерентный прием дискретных символов 78—87
Фазовонекогерентная символьная синхронизация 168—175, 198—200
  , АИМ 204—207, 224, 225
  , символы, имеющие «тонкую струтуру» 251—256
Фазовонекогерентные системы 10
Фазовонекогерентный прием дискретных символов 88—95
Фазовые коды 407—413, 458—461
  без запятой 458—461
  биортогональные 412
  , границы для максимального коэффициента корреляции 408
  , кодирование и декодирование 412—413
  ортогональные 409

ортогональные в фазовокогерентном смысле 409
r-ортогональные 412
, степенная группа 408
трансортогональные 409
Физически реализуемый фильтр 113
Фиксированный объем выборки
, поиск 26—32
Фильтр системы ФАПЧ
, оптимизация 129—136
ФТ 69—72, 97—100 (см. также Фазовая манипуляция)
Q-функция 93

Хаффмана коды 290—293
Хорошо оканчивающаяся i-последовательность 337
Хэмминговская граница 364
Хэмминговские коды 379
, неуязвимость по отношению к потере синхронизации 424—425
Хэмминговское расстояние 358
в сверточных кодах 384—389
в циклических кодах 371
, границы 360—366

Цепи
фильтра оптимизации 129—134
, ширина полосы, 131
Циклические коды без запятой 422—426
Циклические коды, исправляющие ошибки 366—376
, алгебраически синхронизируемые 447—448
, без запятой 422—425
, БЧХ 374—376
, индекс неуязвимости 437—441
, исправляющие и обнаруживающие пачки ошибок, 405—406
, исправляющие ошибки синхронизации 442—447
, максимальной длины 372—373
, минимальное расстояние 371
, неуязвимость по отношению к потере синхронизации 422—423, 425
, перфорированные 377—379
, порождающая матрица 368
, порождающая матрица нуль-пространства 368
, порождающий многочлен 367
, проверочный многочлен 368
, псевдоциклические 377
, укороченные 376—377
, Хэмминга 379

Частичной автокорреляции функция 254
Частичной корреляции коэффициенты 191
Частично самосинхронизирующийся код 303
Частотная манипуляция 95
, символьная синхронизация 211—215, 224—226
Чернова граница 404
ЧТ (см. Частотная манипуляция)

Шум
белый гауссовский 8
небелый гауссовский 75

Элайеса граница 363
Эффективная амплитуда сигнала в системах ФАПЧ 144, 150—151, 218—219
Эффективная оценка 47
Эффективная ширина полосы 56
, АИМ
, когерентный прием 64
, некогерентный прием 69
, ВИМ 97
, ФТ 72
, ЧТ 72
«Эффект квантования» при последовательном поиске 40, 49

ОГЛАВЛЕНИЕ

Стр.
Предисловие редактора перевода 3
Предисловие 4

Часть I

ОСНОВЫ ТЕОРИИ

Глава 1

Синхронные системы связи

1.1. Введение 6
1.2. Модель системы связи 6
1.3. Задача синхронизации 9

Глава 2

Проверка гипотез, теория решений и поиск

2.1. Введение 3
2.2. Выбор между двумя простыми гипотезами 14
2.3. Последовательный тест отношения плотностей вероятностей 18
2.4. Проверка сложных гипотез 22
2.5. Поиск 26
2.6. Последовательный поиск 32
2.7. Об оптимальном последовательном поиске 40
2.8. Проверка многих гипотез 42
2.9. Оценка статистических параметров 45
Задачи 48

Глава 3

Непрерывные по амплитуде и дискретные по времени системы связи

3.1. Введение 51
3.2. Теорема отсчетов 52
3.3. О расчете систем импульсной модуляции 55
3.4. Оптимальная демодуляция 56
3.5. Когерентная амплитудно-импульсная модуляция 61
3.6. Некогерентная по фазе амплитудно-импульсная модуляция 64
3.7. Фазовая манипуляция 69
3.8. Заключительные замечания 72
Задачи 74

Глава 4

Дискретные по амплитуде и по времени системы связи

4.1. Введение 76
4.2. Оптимальный когерентный по фазе приемник и его характеристики . 78
4.3. Некогерентный по фазе прием 88
4.4. Генерирование ортогональных символов 95
4.5. Фазовая манипуляция (ФТ). Когерентный по фазе прием 97
4.6. Фазовая манипуляция. Относительный когерентный прием 100
4.7. Сравнение вероятностей ошибок в бите, символе и слове 105
4.8. Заключительные замечания 109
Задачи 110

Глава 5

Оптимальные фильтры, согласованные фильтры и системы фазовой автоподстройки частоты

5.1. Введение . . . 111
5.2. Оптимальный линейный фильтр . . . 113
5.3. Пересмотр теории согласованных фильтров . . . 121
5.4. Формулы оценок при отслеживании фазы . . . 122
5.5. Линейная модель . . . 126
5.6. Оптимизация фильтра в системе ФАПЧ . . . 129
5.7. Время входа в синхронизм . . . 136
5.8. Системы ФАПЧ и несинусоидальные сигналы . . . 141
Задачи . . . 146

Часть II

СИНХРОНИЗАЦИЯ

Глава 6

Синхронизация по отдельному каналу

6.1. Введение . . . 148
6.2. Синусоидальные сигналы времени . . . 148
6.3. Несинусоидальные сигналы времени . . . 150
6.4. Поиск метки . . . 154
6.5. Оценка меток . . . 163
6.6. Фазовонекогерентная синхронизация . . . 168
6.7. Выбор синхросигнала. Псевдошумовые последовательности . . . 175
6.8. Выбор синхросигнала. Последовательности, быстро входящие в синхронизм . . . 181
6.9. Заключительные замечания . . . 189
Задачи . . . 192

Глава 7

Синхронизация символов по максимуму правдоподобия

7.1. Введение . . . 196
7.2. Символьный синхронизатор максимального правдоподобия . . . 196
7.3. Синхронизация символов АИМ . . . 200
7.4. Символьная синхронизация для ФТ . . . 207
7.5. Синхронизация ортогональных символов . . . 211
7.6. Синхронизаторы, отслеживающие символы . . . 217
7.7. Синхронизация непрямоугольных символов . . . 226
7.8. Заключительные замечания . . . 231
Задачи . . . 232

Глава 8

Синхронизация несущей методом максимального правдоподобия

8.1. Введение . . . 234
8.2. Синхронизация АИМ несущей . . . 235
8.3. Отслеживание фазы ФТ несущей . . . 238
8.4. Отслеживание фазы несущей при большом отношении сигнал/шум . . . 242
8.5. Система Костаса и квадратичная система . . . 246
8.6. Отслеживание символов, имеющих «тонкую структуру» . . . 251
8.7. Заключительные замечания . . . 256
Задачи . . . 256

Глава 9

Задача распределения мощности

9.1. Введение . . . 258
9.2. Влияние неточностей в опорных сигналах. Амплитудно-импульсная модуляция . . . 261
9.3. Влияние неточностей в опорных сигналах. Фазовая манипуляция . . . 263

9.4. Влияние неточностей в опорных сигналах. Ортогональные символы . 270
9.5. Оптимальное распределение мощности 273
9.6. Сравнение синхронизации по отдельному каналу с синхронизацией в случае единого канала 279
9.7. Заключительные замечания 282

Часть III

КОДИРОВАНИЕ

Глава 10

Кодирование источника. Однозначность декодирования

10.1. Введение 284
10.2. Неравенство Крафта и полные словари 287
10.3. Коды Хаффмана 290
10.4. Проверка произвольного словаря на однозначную декодируемость . 293

Глава 11

Синхронизируемость

11.1. Введение 297
11.2. Проверка словаря на синхронизируемость 297
11.3. Самосинхронизирующиеся кодовые словари 302
11.4. Верхняя граница для числа слов в синхронизируемом словаре . . 312
11.5. Максимальные синхронизируемые словари 318

Глава 12

Синхронизируемые блоковые коды

12.1. Введение 326
12.2. Коды без запятой 326
12.3. Коды без запятой с инвариантными путями 331
12.4. Префиксные коды 336
12.5. Коды с запятой 344
12.6. Блоковые коды, синхронизируемые при использовании ФТ . . . 349
12.7. Заключительные замечания 353

Глава 13

Кодирование для устранения ошибок

13.1. Введение 355
13.2. Линейные коды 358
13.3. Границы для минимального расстояния между кодовыми словами . 360
13.4. Циклические коды 366
13.5. Некоторые важные циклические коды 372
13.6. Перфорированные циклические коды, укороченные циклические коды и коды Хэмминга 376
13.7. Кронекеровское произведение, кронекеровская сумма и каскадные коды 379
13.8. Сверточные коды 383
13.9. Кодирование и декодирование линейных кодов 389
13.10. Вероятности ошибочного декодирования 401
13.11. Кодирование для канала с белым гауссовским шумом. Полифазные коды 406

Глава 14

Синхронизируемые коды, исправляющие ошибки

14.1. Введение 414
14.2. Префиксные коды и коды с запятой, исправляющие ошибки . . . 415
14.3. Коды без запятой, исправляющие ошибки 418
14.4. Циклические коды без запятой 422
14.5. Синхронизация в каналах с шумами 426

14.6. Последовательности Баркера 427
14.7. Индекс свободы от запятой 432
14.8. Вычисление индекса неуязвимости смежных классов линейных кодов 435
14.9. Индекс неуязвимости циклических кодов 437
14.10. Коды, исправляющие ошибки синхронизации 442
14.11. Алгебраически синхронизируемые коды, исправляющие ошибки . . 447
14.12. Синхронизируемые коды, исправляющие пачки ошибок 451
14.13. Индекс свободы от запятой в кронекеровском произведении кодов, кронекеровской сумме кодов и в каскадных кодах 454
14.14. Фазовые коды без запятой 458
14.15. Фазовые последовательности Баркера 461
14.16. Синхронизация слов и кадров. Выбор статистик 463
14.17. Синхронизация слов и кадров. Синхронизационная задержка . . 468

Алфавитно-предметный указатель 473

Дж. Дж. Стиффлер

Теория синхронной связи

Пер. с англ. Б. С. Цыбакова
под ред. Э. М. Габидулина

Редактор С. Т. Симонова
Техн. редактор К. Г. Маркоч
Художник А. В. Львов
Корректор Л. Н. Лещева

Сдано в набор 10/XI 1974 г.
Подписано в печ. 10/IV 1975 г.
Форм. 60×90/16 Бумага писч. № 1
30,5 усл.-п. л. 33,25 уч.-изд. л.
Тираж 7 700 экз. Изд. № 16374
Зак. № 281 Цена 2 руб. 90 коп.
Издательство «Связь», Москва 101000,
Чистопрудный бульвар, д. 2

Типография издательства «Связь»
Госкомиздата СССР
Москва 101000, ул. Кирова, д. 40

25.- [illegible]

NAKLADATELSTVÍ [illegible]

2 р. 80 к.

[illegible]

ДЖ. ДЖ. СТИФФЛЕР Теория синхронной связи